



คู่มือการปฏิบัติตามข้อกำหนดการกำกับดูแล
อุตสาหกรรมการเงินของ Tencent
Cloud ในประเทศไทย

เมษายน 2569

【ข้อแถลงเรื่องลิขสิทธิ์】

©2013-2026 Tencent Cloud สงวนลิขสิทธิ์

เอกสารนี้เป็นลิขสิทธิ์ของ Tencent Cloud แต่เพียงผู้เดียว

โดยไม่ได้รับความยินยอมเป็นลายลักษณ์อักษรล่วงหน้าจาก Tencent Cloud ห้ามมิให้บุคคลใด ๆ ทำซ้ำ แก้ไข เลียนแบบ หรือเผยแพร่เนื้อหาทั้งหมดหรือบางส่วนของเอกสารนี้ไม่ว่าในรูปแบบใด

【ข้อแถลงเกี่ยวกับเครื่องหมายการค้า】



Tencent Cloud

เครื่องหมายการค้า รวมถึงเครื่องหมายการค้าอื่น ๆ ที่เกี่ยวข้องกับบริการ

Tencent Cloud เป็นกรรมสิทธิ์ของ Tencent Cloud Computing (Beijing) Co., Ltd.

และบริษัทในเครือ

เครื่องหมายการค้าของบุคคลที่สามซึ่งปรากฏในเอกสารนี้เป็นกรรมสิทธิ์ของเจ้าของตามกฎหมาย

【ข้อแถลงเกี่ยวกับบริการ】

เอกสารนี้จัดทำขึ้นเพื่อวัตถุประสงค์ในการอ้างอิงเท่านั้น Tencent Cloud ไม่ให้การรับรองใด ๆ

ไม่ว่าโดยชัดแจ้งหรือโดยนัย สำหรับข้อมูลในเอกสารนี้ เอกสารนี้จัดทำขึ้นตามสภาพที่มีอยู่ในขณะนั้น ข้อมูลและความคิดเห็นในเอกสารนี้ รวมถึงการอ้างอิงถึง URL และเว็บไซต์อินเทอร์เน็ตอื่น ๆ

อาจมีการเปลี่ยนแปลงโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

ท่านใช้เอกสารนี้โดยรับทราบถึงความเสี่ยงด้วยตนเอง

เอกสารนี้ไม่ได้ให้สิทธิทางกฎหมายในทรัพย์สินทางปัญญาของผลิตภัณฑ์ Tencent ใด ๆ แก่ท่าน

ท่านสามารถคัดลอกและใช้เนื้อหาของเอกสารนี้เพื่อวัตถุประสงค์ในการอ้างอิงภายในองค์กรของท่านเท่านั้น

ตัวอย่างบางส่วนที่อธิบายไว้ในที่นี้มีไว้เพื่อประกอบการอธิบายเท่านั้น และเป็นเรื่องสมมติ

ไม่ควรใช้เป็นพื้นฐานในการอนุมานหรือคาดหมายถึงความสัมพันธ์หรือการเชื่อมโยงใด ๆ

ในความเป็นจริง

STANDARD TENCENT CONTENT

01	บทสรุป	
02	ความปลอดภัยและการปฏิบัติตามข้อกำหนดด้านความ	
	เป็นส่วนตัวของ Tencent Cloud	
2.1	การรับรองระหว่างประเทศที่เป็นที่ยอมรับ	5
2.2	การรับรองระบบ ISO/IEC.....	6
2.3	การรับรองระดับภูมิภาคและอุตสาหกรรม	7
03	โมเดลการแบ่งปันความรับผิดชอบด้านความปลอดภัยของ Tencent Cloud	
04	โครงสร้างพื้นฐานระดับโลกของ Tencent Cloud	
05	Tencent Cloud	
	จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ	
	หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ	
	ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ	
	ของ BOT อย่างไร	
5.1	หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ-	
	เนื้อหาหลัก.....	21
5.1.1	หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ	
		21
5.1.2	การแจ้งการรายงาน หรือการขออนุญาต ต่ออธิบดี.....	26
5.2	เอกสารแนบ 1	
	ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและส	
	ถาบันการเงินเฉพาะกิจ	29
5.3	เอกสารแนบ 2	
	การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ	
	ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ	33
5.4	เอกสารแนบ 3	
	การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการ	
	เงินและสถาบันการเงินเฉพาะกิจ	72
5.5	เอกสารแนบ 4	
	การกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสาร	
	สนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ.....	75
5.6	เอกสารแนบ 5	
	การตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและ	
	สถาบันการเงินเฉพาะกิจ.....	77
5.7	แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก	
		79
5.7.1	การกำกับการดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก	
		79

5.7.2 การบริหารจัดการความเสี่ยงจากบุคคลภายนอก	80
5.7.3 การใช้บริการ public cloud computing กับระบบงานสำคัญ	114

06 Tencent Cloud
จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับหลักเกณฑ์การให้บริการจากผู้ให้บริการภายนอก ของ BOT อย่างไร

07 Tencent Cloud
จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับหลักเกณฑ์การให้บริการจากพันธมิตรทางธุรกิจของสถาบันการเงิน ของ BOT อย่างไร

08 Tencent Cloud
จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับเรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศตามกฎหมายว่าด้วยระบบการชำระเงิน ของ BOT อย่างไร

8.1 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene)	152
8.2 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)	159
8.3 การแจ้งหรือรายงานต่ออปท.	164

09 Tencent Cloud
จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับหลักเกณฑ์ทั่วไปในการกำกับดูแลการประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ ของ BOT อย่างไร

10 Tencent Cloud
จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ BOT อย่างไร

10.1 เรื่องนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ-เนื้อหาหลัก	178
10.2 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงิน.....	181
10.2.1 การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้.....	181
10.2.2 การรักษาความลับของข้อมูลและความถูกต้องเชื่อถือได้ของระบบสารสนเทศ	186
10.2.3 การรักษาสภาพความพร้อมใช้งานของการให้บริการ.....	193

10.2.4 การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ... 204

11 Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ
SEC เรื่อง

ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี
ระบบเทคโนโลยีสารสนเทศ อย่างไร

11.1 เรื่อง

กฎระเบียบอย่างละเอียดในการจัดตั้งระบบเทคโนโลยีสารสนเทศ
.....208

11.2 ภาคผนวก 2

การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ....209

11.3 ภาคผนวก 3

การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ 210

11.4 ภาคผนวก 4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ .257

12 Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ
SEC Cloud Computing Practice อย่างไร

13 Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ
SEC หลักเกณฑ์ เงื่อนไข

และวิธีการในการมอบหมายให้บุคคลอื่น
เป็นผู้รับดำเนินการในงานที่เกี่ยวข้อง
กับการประกอบธุรกิจ อย่างไร

14 Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ
OIC

หลักเกณฑ์การกำกับดูแลและบริหารจัดการความ
เสี่ยงด้านเทคโนโลยีสารสนเทศ อย่างไร

14.1 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ
.....299

14.2 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ 328

14.3

การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยี
สารสนเทศ.....331

14.4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ 332

14.5

การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงป
ลอดภัยไซเบอร์.....334

14.6

การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต
อระบบเทคโนโลยีสารสนเทศ 349

15 ส่วนท้าย

16 ประวัติเวอร์ชัน

01

บทสรุป

ในปัจจุบัน

เทคโนโลยีสารสนเทศได้ถูกผนวกซึ่งเข้ากับระบบการดำเนินงานของสถาบันการเงินจนกลายเป็นโครงสร้างพื้นฐานสำคัญในการเพิ่มประสิทธิภาพการดำเนินงาน ลดต้นทุนการดำเนินงาน เสริมสร้างความสะดวกสบายให้กับลูกค้า และขยายขอบเขตการให้บริการทางการเงิน การใช้เทคโนโลยีสารสนเทศอย่างกว้างขวางนำมาซึ่งแนวโน้มที่หลากหลายและพัฒนาอย่างต่อเนื่องของความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภัยคุกคามทางเครือข่าย และความเสี่ยงจากการฉ้อโกงทางการเงิน หากสถาบันการเงินมีช่องว่างในการจัดการความเสี่ยงทั้งภายในและภายนอก หรือขาดการเตรียมพร้อมที่เพียงพอต่อการโจมตีทางไซเบอร์ อาจนำไปสู่ความเสี่ยงทางธุรกิจ ส่งผลกระทบต่อความต่อเนื่องของบริการและความไว้วางใจของลูกค้า รวมถึงอาจกระทบต่อเสถียรภาพโดยรวมของระบบการเงินได้ เพื่อรับมือกับสิ่งนี้ ธนาคารแห่งประเทศไทย (Bank of Thailand, ต่อไปจะเรียกว่า "ธปท." หรือ "BOT"), สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (The Securities and Exchange Commission, ต่อไปจะเรียกว่า "สำนักงาน ก.ล.ต." หรือ "SEC") และ คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (The Office of Insurance Commission, ต่อไปจะเรียกว่า "สำนักงาน คปภ." หรือ "OIC") ได้กำหนดและเผยแพร่ชุดข้อบังคับด้านกฎระเบียบที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศขึ้น ข้อบังคับเหล่านี้มีวัตถุประสงค์เพื่อชี้นำสถาบันการเงินให้ปรับตัวเข้ากับสภาพแวดล้อมความเสี่ยงและรูปแบบธุรกิจที่เปลี่ยนแปลงอย่างต่อเนื่อง สร้างกลไกการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและความปลอดภัยทางเครือข่ายอย่างเป็นระบบที่มีมั่นคงแข็งแรง รับประกันความปลอดภัย ความมั่นคง และการปฏิบัติตามกฎระเบียบของการประยุกต์ใช้เทคโนโลยีสารสนเทศ เพื่อธำรงการทำงานที่มีมั่นคงของระบบการเงิน

Tencent Cloud

ติดตามความเคลื่อนไหวล่าสุดและการเผยแพร่ข้อมูลอย่างเป็นทางการด้านกฎระเบียบของธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยอย่างต่อเนื่อง และมุ่งมั่นที่จะช่วยเหลือลูกค้าสถาบันการเงินในประเทศไทยให้ปฏิบัติตามข้อกำหนดทางกฎระเบียบ เอกสารนี้จะอธิบายว่า Tencent Cloud สามารถช่วยเหลือลูกค้าในการปฏิบัติตามข้อกำหนดทางกฎระเบียบได้อย่างไร โดยมุ่งเน้นที่แนวทางและประกาศกำกับดูแลต่อไปนี้ซึ่งเป็นที่สนใจอย่างยิ่งของสถาบันการเงิน:

ธนาคารแห่งประเทศไทย (Bank of Thailand, BOT) :

- [BOT No. Sor Gor Chor 5/2566 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ \(Information Technology risk\) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ](#)
- [BOT No. FPG 8/2557 เรื่อง หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก \(Outsourcing\)](#)
- [BOT No. FPG 16/2563 เรื่อง หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจ \(business partner\) ของสถาบันการเงิน](#)

- [BOT No. SorNorChor 1/2564](#)
[เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ \(Information Technology Risk\) ตามกฎหมายว่าด้วยระบบการชำระเงิน](#)
- [BOT No. SorNorChor 6/2561 เรื่อง หลักเกณฑ์ทั่วไปในการกำกับดูแล](#)
[การประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ](#)
- [BOT No. SorNorChor 11/2561 เรื่อง](#)
[นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ](#)

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (The Securities and Exchange Commission, SEC) :

- [SEC No. Sor Thor 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี](#)
[ระบบเทคโนโลยีสารสนเทศ](#)
- [SEC No. Nor Thor 33/2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี](#)
[ระบบเทคโนโลยีสารสนเทศ](#)
- [Cloud Computing Practice](#)
- [SEC No. Tor Thor 60/2561 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการในการมอบหมายให้บุคคลอื่น](#)
[เป็นผู้รับดำเนินการในงานที่เกี่ยวข้องกับการประกอบธุรกิจ](#)

คณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (The Office of Insurance Commission, OIC) :

- [OIC B.E. 2563 เรื่อง](#)
[หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของบริษัทประกัน](#)
[ชีวิต](#)
- [OIC B.E. 2563 เรื่อง](#)
[หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ](#)
[ของบริษัทประกันวินาศภัย](#)

02

ความปลอดภัยและการป ฏิบัติตามข้อกำหนดด้าน ความเป็นส่วนตัวของ Tencent Cloud

การปฏิบัติตามข้อกำหนด (Compliance) เป็นรากฐานของการพัฒนาของ Tencent Cloud Tencent Cloud ระบุและนำมาตรฐานความปลอดภัยระดับสากลและมาตรฐานอุตสาหกรรมชั้นนำมาใช้ ปฏิบัติตามข้อกำหนดด้านการปฏิบัติตามข้อกำหนดของประเทศ/ภูมิภาคและอุตสาหกรรมต่างๆ ปรับปรุงระบบการจัดการภายในอย่างต่อเนื่อง ยกกระดับความสามารถในการควบคุมความปลอดภัยของ Tencent Cloud และทุ่มเทสร้างบริการคลาวด์ที่น่าเชื่อถือสำหรับลูกค้า ในเวลาเดียวกัน Tencent Cloud ยังมีส่วนร่วมอย่างแข็งขันในการกำหนดและเผยแพร่มาตรฐานความปลอดภัยของอุตสาหกรรม ดำเนินนโยบาย "การปฏิบัติตามข้อกำหนดคือบริการ" (Compliance as a Service) และสร้างและดำเนินระบบนิเวศคลาวด์ที่ปลอดภัยและน่าเชื่อถือ

จนถึงปัจจุบัน Tencent Cloud

ได้รับการรับรองและคุณวุฒิด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดเป็นส่วนตัวหลายรายการผ่านการตรวจสอบหรือการประเมินโดยบุคคลที่สามที่เป็นอิสระ

ซึ่งพิสูจน์ว่าการจัดการความปลอดภัยและการสร้างการปกป้องความเป็นส่วนตัวของ Tencent Cloud เป็นไปตามมาตรฐานการรับรองที่เกี่ยวข้องหรือแนวปฏิบัติที่ดีของอุตสาหกรรม

หากต้องการทราบข้อมูลเพิ่มเติมเกี่ยวกับการปฏิบัติตามข้อกำหนดของ Tencent Cloud โปรดดูที่หน้า [Tencent Cloud Compliance Center](#)

หากต้องการใบรับรองหรือรายงานการปฏิบัติตามข้อกำหนดที่เกี่ยวข้อง โปรดสมัครและดาวน์โหลดผ่าน [Compliance Document Download](#)

ต่อไปนี้เป็นตัวอย่างของการรับรองระหว่างประเทศที่ได้รับการยอมรับในระดับสากลและการยอมรับในระดับภูมิภาคและอุตสาหกรรมบางส่วนของ Tencent Cloud:

2.1 การรับรองระหว่างประเทศที่เป็นที่ยอมรับ

CSA STAR	การประเมินความปลอดภัยคลาวด์ STAR เป็นการรับรองระดับนานาชาติที่มุ่งเน้นคุณลักษณะด้านความปลอดภัยของคลาวด์ ซึ่งพัฒนาโดย Cloud Security Alliance (CSA) องค์กรไม่แสวงหาผลกำไรที่เป็นที่ยอมรับในระดับโลก การรับรองนี้ได้ขยายระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001 ออกไป และผสมผสานกับเมทริกซ์ควบคุมความปลอดภัยคลาวด์ (Cloud Control Matrix, CCM) เพื่อทำให้ปัญหาที่เฉพาะเจาะจงของความปลอดภัยคลาวด์สามารถมองเห็นได้ ช่วยให้ผู้ใช้มีภาพรวมการประเมินโครงสร้างความปลอดภัยที่เข้าใจได้โดยง่าย ด้วยประสบการณ์ด้านความปลอดภัยที่ Tencent สั่งสมมาหลายปี Tencent Cloud ได้รับการรับรองความปลอดภัยคลาวด์ระดับ Gold ระดับโลกจาก CSA STAR ซึ่งแสดงให้เห็นว่าระบบควบคุมความปลอดภัยของ Tencent Cloud เป็นไปตามมาตรฐานความปลอดภัยคลาวด์ที่เป็นที่ยอมรับในระดับสากล
การตรวจสอบ SOC	รายงานการควบคุมระบบและองค์กร (System and Organization Controls Reports หรือที่เรียกว่า "รายงาน SOC") เป็นชุดรายงานที่เกี่ยวข้องกับการควบคุมภายในของผู้ให้บริการ ซึ่งจัดทำโดยบริษัทสอบบัญชีบุคคลที่สามมีอาชีพตามหลักเกณฑ์ที่เกี่ยวข้องของ American Institute of Certified Public Accountants (AICPA) รายงาน SOC ในฐานะรายงานการตรวจสอบอิสระ ครอบคลุมจุดควบคุมที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับของแพลตฟอร์ม Tencent Cloud ตามประเภทบริการการรับรองที่แตกต่างกัน รายงาน SOC สามารถจัดเตรียมให้กับผู้ใช้คลาวด์และผู้ตรวจสอบของพวกเขา เพื่อให้ข้อมูลที่มีคุณค่าแก่ผู้ใช้ Tencent Cloud สำหรับการประเมินและจัดการความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการ

2.2 การรับรองระบบ ISO/IEC

การรับรอง ISO/IEC 22301: 2019	ISO/IEC 22301: 2019 เป็นมาตรฐานสากลที่มีหัวข้อหลักเกี่ยวกับการจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ซึ่งให้วิธีการ BCM ที่สมบูรณ์และเป็นสากล มีวัตถุประสงค์เพื่อช่วยองค์กรในการระบุและตอบสนองต่อเหตุการณ์ที่อาจก่อให้เกิดความเสียหาย เพื่อรับประกันความต่อเนื่องของการดำเนินงานที่สำคัญ ลดความเสี่ยง และปกป้ององค์กรจากผลกระทบที่รุนแรง Tencent Cloud ได้รับการรับรอง ISO/IEC 22301: 2019 แล้ว ซึ่งพิสูจน์ว่า Tencent Cloud ได้สร้างกระบวนการจัดการความต่อเนื่องทางธุรกิจที่เป็นทางการ เพื่อรับประกันความต่อเนื่องและความเสถียรของธุรกิจของตนเอง
การรับรอง ISO/IEC 27001: 2022	ISO/IEC 27001: 2022 เป็นมาตรฐานการรับรองระบบที่ได้รับการยอมรับอย่างกว้างขวาง มีความเข้มงวด และเป็นที่ยอมรับมากที่สุดในระดับสากลสำหรับด้านความปลอดภัยข้อมูล การผ่านการรับรองนี้หมายความว่าองค์กรได้สร้างระบบการจัดการความปลอดภัยข้อมูลที่วิทยาศาสตร์และมีประสิทธิภาพเพื่อประสานกลยุทธ์การพัฒนางานองค์กรกับการจัดการความปลอดภัยข้อมูลและรับประกันว่าความเสี่ยงด้านความปลอดภัยข้อมูลที่เกี่ยวข้องได้รับการควบคุม และจัดการอย่างเหมาะสม การผ่านการรับรอง ISO/IEC 27001: 2022 สามารถแสดงให้เห็นถึงความมุ่งมั่นด้านความปลอดภัยของ Tencent Cloud ได้ดียิ่งขึ้น ซึ่งให้เห็นว่า Tencent Cloud ได้สร้างระบบการจัดการที่วิทยาศาสตร์และมีประสิทธิภาพ ซึ่งสามารถจัดเตรียมผลิตภัณฑ์และบริการคลาวด์ที่ปลอดภัยและน่าเชื่อถือให้กับผู้ใช้ได้
การรับรอง ISO/IEC 20000-1: 2018	ISO/IEC 20000-1: 2018 เป็นชุดมาตรฐานสากลที่กำหนดขึ้นสำหรับการจัดการบริการด้านเทคโนโลยีสารสนเทศ ระบบนี้ควบคุมการจัดการบริการเทคโนโลยีสารสนเทศขององค์กร ตั้งแต่รูปแบบการสร้าง การนำไปปฏิบัติ การดำเนินงาน การตรวจสอบ การทบทวน การบำรุงรักษา และการปรับปรุง ช่วยให้องค์กรสามารถระบุและจัดการปัญหาด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องอย่างต่อเนื่อง เสริมสร้างการสื่อสารกับผู้ใช้ และสร้างระบบบริการที่เป็นมาตรฐานที่สามารถปรับปรุงตนเองได้อย่างต่อเนื่อง Tencent Cloud ได้รับการรับรอง ISO/IEC 20000-1: 2018 แล้ว ซึ่งครอบคลุมขอบเขตการรับรอง เช่น บริการคอมพิวเตอร์คลาวด์ บริการโฮสติ้ง และบริการกู้คืนจากภัยพิบัติ Tencent Cloud ปฏิบัติตามทัศนคติที่ให้ความสำคัญกับการบริการเป็นอันดับหนึ่งอย่างเคร่งครัด ปรับปรุงกลไกการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารกับลูกค้า
การรับรอง ISO/IEC 9001: 2015	ISO/IEC 9001: 2015 เป็นระบบการจัดการคุณภาพที่ได้รับการยอมรับอย่างกว้างขวางในระดับสากลและเป็นที่ครอบคลุมทั่วระบบนี้ให้กรอบการจัดการคุณภาพและข้อกำหนดเชิงแนะนำสำหรับกระบวนการทั้งหมดของการให้ผลิตภัณฑ์หรือบริการขององค์กรใช้เพื่อช่วยองค์กรในการรักษาผลิตภัณฑ์หรือบริการ รับประกันคุณภาพการส่งมอบที่เสถียรและสม่ำเสมอ Tencent Cloud ได้รับการรับรอง ISO/IEC 9001: 2015 แล้ว โดยครอบคลุมบริการ เช่น บริการคอมพิวเตอร์คลาวด์ บริการโฮสติ้ง และบริการกู้คืนจากภัยพิบัติ Tencent Cloud บรรลุเป้าหมายคุณภาพที่คาดหวังได้อย่างมีประสิทธิภาพและประสิทธิผลผ่านการใช้ระบบการจัดการคุณภาพ และรับประกันคุณภาพและการดำเนินงานของผลิตภัณฑ์และบริการคลาวด์
การรับรอง ISO/IEC 27017: 2015	ISO/IEC 27017: 2015 เป็นส่วนเสริมของ ISO/IEC 27002: 2013 และเป็นมาตรฐานปฏิบัติสำหรับความปลอดภัยข้อมูลของบริการคลาวด์ ซึ่งให้การควบคุมความปลอดภัยเฉพาะและแนวทางการนำไปปฏิบัติสำหรับผู้ให้บริการคลาวด์

	และลูกค้าเสริมสร้างการควบคุมภัยคุกคามและความเสี่ยงจากช่องโหว่ในการประมวลผลแบบคลาวด์ Tencent Cloud ได้รับการรับรอง ISO/IEC 27017: 2015 แล้ว ซึ่งไม่เพียงแต่แสดงว่า Tencent Cloud จะใช้แนวปฏิบัติที่ดีที่สุดที่ได้รับการยอมรับในระดับสากลอย่างต่อเนื่อง แต่ยังพิสูจน์ว่า Tencent Cloud ได้สร้างระบบการจัดการความปลอดภัยคลาวด์ที่ครอบคลุมมากขึ้น และยกระดับความสามารถในการให้บริการความปลอดภัยคลาวด์โดยรวม
การรับรอง ISO/IEC 27018: 2014	ISO/IEC 27018: 2014 เป็นมาตรฐานความปลอดภัยที่ครอบคลุมและเป็นที่ยอมรับในระดับโลกมากที่สุดสำหรับการประมวลผลข้อมูลที่สามารถระบุตัวบุคคล (PII) ในสภาพแวดล้อมคลาวด์สาธารณะ มาตรฐานนี้มีวัตถุประสงค์เพื่อจัดเตรียมชุดแนวปฏิบัติสำหรับการปกป้องความเป็นส่วนตัวของผู้ใช้ให้แก่ผู้ให้บริการคลาวด์ เพื่อรับประกันความปลอดภัยของข้อมูลส่วนบุคคลในสภาพแวดล้อมคอมพิวเตอร์คลาวด์ Tencent Cloud ได้รับการรับรอง ISO/IEC 27018: 2014 แล้ว ซึ่งบ่งชี้ว่าระบบการจัดการข้อมูลส่วนบุคคลของ Tencent Cloud สอดคล้องกับกฎระเบียบการปกป้องข้อมูลส่วนบุคคลที่เข้มงวดในระดับสากลและให้ความไว้วางใจและการรับประกันเพิ่มเติมเกี่ยวกับความปลอดภัยบนคลาวด์ให้แก่ลูกค้าของ Tencent Cloud
การรับรอง ISO/IEC 29151: 2017	ISO/IEC 29151: 2017 เป็นมาตรฐานสากลที่ใช้สำหรับดำเนินการควบคุมเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลที่สามารถระบุตัวตน (PII) เพื่อให้เป็นไปตามข้อกำหนดที่กำหนดโดยการประเมินความเสี่ยงและผลกระทบด้านความเป็นส่วนตัวที่เกี่ยวข้องกับการปกป้อง PII Tencent Cloud ได้รับการรับรอง ISO/IEC 29151: 2017 แล้ว ซึ่งแสดงว่า Tencent Cloud ได้พัฒนาระบบควบคุมความปลอดภัยที่เหมาะสมตามเป้าหมาย PII และความต้องการทางธุรกิจของตน จัดเตรียมการควบคุมการปกป้องความเป็นส่วนตัวในระดับสูงสำหรับ PII ของผู้ใช้บนคลาวด์
การรับรอง ISO/IEC 27701: 2019	ISO/IEC 27701: 2019 ซึ่งเป็นข้อกำหนดและแนวทางการขยายของ ISO/IEC 27001 และ ISO/IEC 27002 ในการจัดการข้อมูลส่วนบุคคล (Privacy Information Management) ให้คำแนะนำสำหรับการสร้าง การนำไปปฏิบัติ การบำรุงรักษา และการปรับปรุงระบบการจัดการข้อมูลส่วนบุคคลอย่างต่อเนื่อง ถือเป็นจุดสำคัญของการจัดการความเสี่ยงด้านความเป็นส่วนตัวอย่างต่อเนื่อง Tencent Cloud ได้รับการรับรอง ISO/IEC 27701: 2019 แล้ว ซึ่งพิสูจน์ว่า Tencent Cloud ยึดถือการปกป้องความเป็นส่วนตัวของผู้ใช้เป็นหัวใจหลักของการให้บริการเสมอมา และแสดงให้เห็นอย่างชัดเจนถึงมาตรฐานและความน่าเชื่อถือของการปกป้องความเป็นส่วนตัวของผลิตภัณฑ์ Tencent Cloud

2.3 การรับรองระดับภูมิภาคและอุตสาหกรรม

C5 ของเยอรมนี	แคตตาล็อกเกณฑ์การปฏิบัติตามข้อกำหนดสำหรับระบบคลาวด์ (Cloud Computing Compliance Criteria Catalogue, เรียกว่า C5) ได้รับการกำหนดโดยสำนักงานความปลอดภัยข้อมูลแห่งสหพันธ์สาธารณรัฐเยอรมนี (Federal Office for Information Security, BSI) มีวัตถุประสงค์เพื่อตรวจสอบการปฏิบัติตามข้อกำหนดด้านความปลอดภัยข้อมูลของผู้ให้บริการคลาวด์โดยอิงตามการตรวจสอบและการรายงานที่เป็นมาตรฐาน C5 เป็นมาตรฐานความปลอดภัยระดับสูงที่ได้รับการยอมรับอย่างกว้างขวางในวงการอุตสาหกรรมบริการคลาวด์

	Tencent Cloud ผ่านเกณฑ์การตรวจสอบพื้นฐานและเพิ่มเติมของ C5: 2020 ของเยอรมนีแล้ว ซึ่งหมายความว่า Tencent Cloud มีมาตรฐานสูงที่กำหนดโดยรัฐบาลเยอรมนีในด้านการปกป้องข้อมูลและความปลอดภัยข้อมูล
TISAX ของเยอรมนี	TISAX เป็นมาตรฐานการประเมินความปลอดภัยข้อมูลและความปลอดภัยในการแลกเปลี่ยนข้อมูลสำหรับอุตสาหกรรมยานยนต์ ซึ่งพัฒนาโดยสภาอุตสาหกรรมยานยนต์เยอรมัน (VDA) ร่วมกับสมาคมการแลกเปลี่ยนข้อมูลความปลอดภัยอุตสาหกรรมยานยนต์ยุโรป (ENX) TISAX ทำให้การประเมินความปลอดภัยข้อมูลภายในอุตสาหกรรมยานยนต์ได้รับการยอมรับซึ่งกันและกัน และจัดเตรียมกลไกการประเมินและการแลกเปลี่ยนที่เป็นมาตรฐาน ปัจจุบัน ศูนย์ข้อมูลอินเทอร์เนต (IDC) หลายแห่งของ Tencent Cloud (รวมถึงที่ตั้งอยู่ในปักกิ่ง เซินเจิ้น และอื่นๆ) ได้ผ่านการประเมินระดับ 3 ของ TISAX แล้ว ซึ่งหมายความว่าบริการที่ปรับใช้ในภูมิภาคเหล่านี้เป็นไปตามข้อกำหนดของ TISAX และได้สร้างและบำรุงรักษาระบบการจัดการความปลอดภัยข้อมูลที่สมบูรณ์แล้ว
การรับรองระดับ MTCS T3 ของสิงคโปร์	มาตรฐานความปลอดภัยแบบหลายชั้นสำหรับคลาวด์ของสิงคโปร์ (Multi-Tier Cloud Security: MTCS) ได้รับการจัดทำภายใต้การกำกับดูแลของคณะกรรมการมาตรฐานเทคโนโลยีสารสนเทศ (ITSC) ของสำนักงานพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารแห่งสิงคโปร์ (Infocomm Media Development Authority: IMDA) MTCS ในฐานะมาตรฐานทั่วไปสำหรับคลาวด์ ผู้ให้บริการคลาวด์สามารถนำมาใช้เพื่อแก้ไขข้อกังวลของลูกค้าเกี่ยวกับความปลอดภัยและความลับของข้อมูลบนคลาวด์ รวมถึงผลกระทบของการใช้บริการคลาวด์ต่อธุรกิจ Tencent Cloud ได้รับการรับรองมาตรฐานระดับ T3 ของ MTCS ของสิงคโปร์เรียบร้อยแล้ว การรับรองนี้หมายความว่า Tencent Cloud ได้ใช้กลไกการจัดการความเสี่ยงที่มั่นคงและบริการคลาวด์ที่ปลอดภัย เพื่อรับประกันความปลอดภัย ความลับ และความโปร่งใสในการดำเนินงานที่สามารถตรวจสอบได้ของข้อมูลลูกค้าบนคลาวด์
OSPAR ของสิงคโปร์	รายงานการตรวจสอบผู้ให้บริการงานจ้างทำภายนอก (Outsourced Service Providers Audit Report: OSPAR) เป็นมาตรฐานการเข้าสู่ตลาดสำหรับบริการจ้างทำภายนอกในอุตสาหกรรมการเงินของสิงคโปร์ มาตรฐานนี้ใช้ SSAE 3000 ของสิงคโปร์เป็นพื้นฐาน มีวัตถุประสงค์เพื่อตรวจสอบการออกแบบการควบคุมที่เกี่ยวข้องและประสิทธิภาพในการดำเนินงานในสามด้านสำหรับผู้ให้บริการแก่องค์กรการเงินในสิงคโปร์ ได้แก่ การควบคุมในระดับองค์กร การควบคุมเทคโนโลยีสารสนเทศทั่วไป และการควบคุมบริการผลิตภัณฑ์และบริการหลายรายการของ Tencent Cloud ได้ผ่านการตรวจสอบ OSPAR ของสิงคโปร์แล้ว และพยายามอย่างต่อเนื่องเพื่อให้แน่ใจว่าการควบคุมของตนสอดคล้องกับแนวทางของ ABS การผ่านการตรวจสอบนี้แสดงให้เห็นว่าความสามารถด้านความปลอดภัยของ Tencent Cloud เป็นไปตามข้อกำหนดที่เข้มงวดสำหรับบริการทางการเงินของสิงคโปร์และแม้แต่ภูมิภาคเอเชียตะวันออกเฉียงใต้
ตราสัญลักษณ์ความไว้วางใจด้านการปกป้องข้อมูล	ตราสัญลักษณ์ความไว้วางใจด้านการปกป้องข้อมูล (DPTM) ของสิงคโปร์ ได้รับการกำหนดโดยคณะกรรมการปกป้องข้อมูลส่วนบุคคล (Personal Data Protection Commission: PDPC) และสำนักงานพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารแห่งสิงคโปร์ (Infocomm

Protection Trustmark: DPTM) ของสิงคโปร์	Media Media Development Authority: IMDA) ของสิงคโปร์ มีวัตถุประสงค์เพื่อให้องค์กรแสดงให้เห็นถึงแนวปฏิบัติในการปกป้องข้อมูลที่ได้รับผิดชอบ Tencent Cloud ได้รับการรับรองตราสัญลักษณ์ความไว้วางใจด้านการปกป้องข้อมูล (DPTM) ของสิงคโปร์แล้ว ซึ่งบ่งชี้ว่า Tencent Cloud ได้นำแนวปฏิบัติในการปกป้องข้อมูลที่ได้รับผิดชอบไปใช้สำหรับลูกค้า พันธมิตรทางธุรกิจ และหน่วยงานกำกับดูแล และมีความสามารถในการปกป้องข้อมูลส่วนบุคคลที่รวบรวมไว้
Cyber Trust Mark (CTM) สิงคโปร์	Cyber Trust Mark (CTM) คือการรับรองด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติที่ริเริ่มโดยหน่วยงานความมั่นคงปลอดภัยไซเบอร์แห่งสิงคโปร์ (Cyber Security Agency/CSA) กรอบการทำงาน CTM ใช้วิธีการที่อิงตามความเสี่ยง ครอบคลุม 22 โดเมนย่อยใน 4 ด้านหลัก ได้แก่ ธรรมาภิบาลและการบริหารความเสี่ยง การปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ ความยืดหยุ่น ความมั่นคงของห่วงโซ่อุปทานและบุคลากร ตลอดจนการปรับปรุงอย่างต่อเนื่องและแนวปฏิบัติชั้นนำ Tencent Cloud ได้รับการรับรองในระดับสูงสุด (Tier 5) ของ Cyber Trust Mark (CTM) การรับรองดังกล่าวเป็นเครื่องยืนยันถึงความสามารถขั้นสูงของ Tencent Cloud ในด้านธรรมาภิบาลความมั่นคงปลอดภัยไซเบอร์ การบริหารความเสี่ยง และความยืดหยุ่นในการดำเนินงาน อีกทั้งยังส่งเสริมให้ Tencent Cloud เป็นผู้ให้บริการคลาวด์ที่น่าเชื่อถือสำหรับภาคส่วนที่อยู่ภายใต้การกำกับดูแลและมีความต้องการสูงทั่วภูมิภาคเอเชียแปซิฟิก
การรับรอง KISMS ของเกาหลีใต้	การรับรองระบบการจัดการการคุ้มครองความปลอดภัยข้อมูลของเกาหลี (K-ISMS) เป็นการรับรองความปลอดภัยข้อมูลที่ได้รับการสนับสนุนจากรัฐบาลเกาหลีใต้ มีวัตถุประสงค์เพื่อช่วยให้องค์กรและบริษัทในเกาหลีใต้สามารถปกป้องสินทรัพย์ข้อมูลของตนอย่างปลอดภัยและสม่ำเสมอ ตามกฎหมายเทคโนโลยีสารสนเทศและการสื่อสารของเกาหลีใต้ที่เกี่ยวข้อง การที่ Tencent Cloud ได้รับการรับรอง KISMS หมายความว่า ลูกค้าบนคลาวด์ในเกาหลีใต้สามารถพิสูจน์ได้ง่ายขึ้นว่าตนปฏิบัติตามข้อกำหนดทางกฎหมายในท้องถิ่น ซึ่งช่วยปกป้องสินทรัพย์ข้อมูลดิจิทัลที่สำคัญ และยังหมายความว่ามาตรการตอบสนองต่อความปลอดภัยข้อมูลและความสามารถของชั้นตอนการรับมือกับภัยคุกคามของ Tencent Cloud ได้รับการยกระดับขึ้น ซึ่งสามารถลดผลกระทบจากช่องโหว่ด้านความปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น
การตรวจสอบการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศสำหรับอุตสาหกรรมการเงินของมาเลเซีย	หน่วยงานกำกับดูแลทางการเงินของมาเลเซีย เช่น ธนาคารกลางมาเลเซีย (Bank Negara Malaysia: BNM) และคณะกรรมการหลักทรัพย์มาเลเซีย (Securities Commission Malaysia: SC) ได้ออกกฎระเบียบและข้อกำหนดที่เกี่ยวข้องสำหรับอุตสาหกรรมบริการทางการเงิน เพื่อควบคุมการใช้เทคโนโลยีสารสนเทศในบริการทางการเงินของมาเลเซีย เช่น ธนาคาร ประกันภัย และหลักทรัพย์ เพื่อรับประกันความน่าเชื่อถือ ความปลอดภัย และความเสถียรของระบบสารสนเทศทางการเงิน การที่ Tencent Cloud ผ่านการตรวจสอบโดยบุคคลที่สามที่เป็นอิสระสามารถพิสูจน์ได้ว่า บริการคลาวด์ที่ Tencent Cloud ให้แก่ลูกค้าด้านการเงินในมาเลเซียปฏิบัติตามข้อกำหนดด้านกฎระเบียบของอุตสาหกรรมการเงินของมาเลเซียอย่างเคร่งครัด
การตรวจสอบการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศ	หน่วยงานกำกับดูแลทางการเงินของเขตบริหารพิเศษฮ่องกง ได้แก่ หน่วยงานกำกับดูแลทางการเงินฮ่องกง (Hong Kong Monetary Authority: HKMA), คณะกรรมการกำกับหลักทรัพย์และสัญญาซื้อขายล่วงหน้าฮ่องกง (Securities and Futures Commission: SFC) และสำนักงานคณะกรรมการกำกับกิจการประกันภัยฮ่องกง (Insurance Authority: IA)

สำหรับอุตสาหกรรมการเงินของฮ่องกง	ได้ออกข้อกำหนดด้านกฎระเบียบที่สำคัญหลายประการ เพื่อควบคุมการประยุกต์ใช้เทคโนโลยีสารสนเทศในสถาบันการเงิน ประกันภัย และหลักทรัพย์ การที่ Tencent Cloud ผ่านการตรวจสอบโดยบุคคลที่สามที่เป็นอิสระพิสูจน์ว่า Tencent Cloud เป็นผู้ให้บริการคลาวด์ที่น่าเชื่อถือสำหรับอุตสาหกรรมการเงิน Tencent Cloud ได้ใช้แนวทางเชิงรุกในการปฏิบัติตามภาระหน้าที่ด้านการปฏิบัติตามข้อกำหนดที่เข้มงวดที่สุด สถาบันการเงินสามารถสร้างบริการทางการเงินรุ่นต่อไปของตนบน Tencent Cloud ได้อย่างมั่นใจ
การตรวจสอบการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศสำหรับอุตสาหกรรมการเงินของประเทศไทย	สถาบันการเงินในประเทศไทยจำเป็นต้องปฏิบัติตามกฎระเบียบและข้อกำหนดที่เกี่ยวข้องที่ออกโดยหน่วยงานกำกับดูแลทางการเงินและหน่วยงานกฎหมายที่เกี่ยวข้อง เช่น ธนาคารแห่งประเทศไทย (Bank of Thailand: BOT), สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (Office of the Securities and Exchange Commission: OSEC) และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (Office of Insurance Commission: OIC) ข้อกำหนดด้านกฎระเบียบครอบคลุม: การจัดการความเสี่ยงในการใช้เทคโนโลยีสารสนเทศ การปกป้องข้อมูลส่วนบุคคล การใช้และการควบคุมความปลอดภัยของเทคโนโลยีสารสนเทศในระบบต่างๆ เช่น ธนาคาร ประกันภัย ระบบรัฐบาลอิเล็กทรอนิกส์ เงินอิเล็กทรอนิกส์ โครงสร้างพื้นฐานระบบการชำระเงิน ให้บริการบริการชำระเงิน เป็นต้น การที่ Tencent Cloud ผ่านการตรวจสอบโดยบุคคลที่สามที่เป็นอิสระสามารถพิสูจน์ได้ถึงความสามารถของ Tencent Cloud ในการปฏิบัติตามข้อกำหนดด้านกฎระเบียบที่เข้มงวดของอุตสาหกรรมการเงินไทย และความมุ่งมั่นของ Tencent Cloud ในการให้บริการคลาวด์ที่ยืดหยุ่นและเป็นไปตามข้อกำหนดแก่ลูกค้าอุตสาหกรรมการเงินของไทย
การตรวจสอบการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศสำหรับอุตสาหกรรมการเงินของอินโดนีเซีย	หน่วยงานกำกับดูแลทางการเงินของอินโดนีเซีย เช่น ธนาคารกลางอินโดนีเซีย (Bank Indonesia) และสำนักงานบริการทางการเงิน (Otoritas Jasa Keuangan: OJK) ได้ออกกฎระเบียบและข้อกำหนดที่เกี่ยวข้องสำหรับอุตสาหกรรมบริการทางการเงิน ข้อกำหนดด้านกฎระเบียบครอบคลุม: การจัดการความเสี่ยงในการใช้เทคโนโลยีสารสนเทศ การปกป้องข้อมูลส่วนบุคคล การใช้และการควบคุมความปลอดภัยของเทคโนโลยีสารสนเทศในระบบต่างๆ เช่น ธนาคาร ประกันภัย ระบบรัฐบาลอิเล็กทรอนิกส์ เงินอิเล็กทรอนิกส์ โครงสร้างพื้นฐานระบบการชำระเงิน ผู้ให้บริการบริการชำระเงิน เป็นต้น Tencent Cloud ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนดทางการเงินของอินโดนีเซียที่ดำเนินการโดยสถาบันตรวจสอบบุคคลที่สามที่เป็นอิสระ ซึ่งพิสูจน์ว่าบริการคลาวด์ที่ Tencent Cloud ให้แก่ลูกค้าด้านการเงินในอินโดนีเซียปฏิบัติตามข้อกำหนดด้านกฎระเบียบของอุตสาหกรรมการเงินอินโดนีเซียอย่างเคร่งครัด
การตรวจสอบการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศสำหรับอุตสาหกรรมการเงิน	สถาบันการเงินในฟิลิปปินส์จำเป็นต้องปฏิบัติตามกฎระเบียบและข้อกำหนดที่เกี่ยวข้องที่กำหนดโดยหน่วยงานกำกับดูแลทางการเงินและหน่วยงานกฎหมายที่เกี่ยวข้อง เช่น ธนาคารกลางฟิลิปปินส์ (Bangko Sentral ng Pilipinas: BSP) ข้อกำหนดด้านกฎระเบียบครอบคลุม: การจัดการความเสี่ยงในการใช้เทคโนโลยีสารสนเทศ การปกป้องข้อมูลส่วนบุคคล การใช้และการควบคุมความปลอดภัยของเทคโนโลยีสารสนเทศในระบบต่างๆ เช่น ธนาคาร ประกันภัย ระบบรัฐบาลอิเล็กทรอนิกส์ เงินอิเล็กทรอนิกส์ โครงสร้างพื้นฐานระบบการชำระเงิน ผู้ให้บริการบริการชำระเงิน เป็นต้น

นของฟิลิปปินส์	การที่ Tencent Cloud ผ่านการตรวจสอบโดยบุคคลที่สามที่เป็นอิสระสามารถพิสูจน์ได้ถึงความสามารถของ Tencent Cloud ในการปฏิบัติตามข้อกำหนดด้านกฎระเบียบที่เข้มงวดของอุตสาหกรรมการเงินฟิลิปปินส์ และความมุ่งมั่นของ Tencent Cloud ในการให้บริการคลาวด์ที่ยืดหยุ่นและเป็นไปตามข้อกำหนดแก่ลูกค้าอุตสาหกรรมการเงิน
สมาคมภาพยนตร์อเมริกัน (Motion Picture Association of America: MPAA)	สมาคมภาพยนตร์อเมริกัน (MPAA) ได้กำหนดชุดมาตรฐานแนวปฏิบัติที่ดีที่สุดสำหรับการจัดเก็บ ประมวลผล และส่งเนื้อหาสื่อที่มีการป้องกัน คู่มือการดำเนินงานนี้มีวัตถุประสงค์เพื่อให้แอปพลิเคชันและผู้ให้บริการคลาวด์ที่ทำงานร่วมกับสมาชิกของ MPAA ทราบถึงข้อกำหนดที่ควรปฏิบัติตามในด้านความปลอดภัยของเนื้อหา องค์ประกอบของเทมเพลตความปลอดภัยเนื้อหาของ MPAA อ้างอิงมาตรฐาน ISO ที่เกี่ยวข้อง (27001-27002), มาตรฐานความปลอดภัย (เช่น NIST, CSA, ISACA และ SANS) และแนวปฏิบัติที่ดีที่สุดของอุตสาหกรรม Tencent Cloud ได้รับการรับรองที่เกี่ยวข้อง เช่น ISO 27001, ISO 27017, ISO 27018, PCI DSS และ CSA STAR แล้ว และ Tencent Cloud ได้ผ่านการประเมินตนเอง เพื่อให้มั่นใจว่าขั้นตอนการจัดการเนื้อหาของลูกค้าของตนเป็นไปตามแนวทางโมเดลความปลอดภัยเนื้อหาของสมาคมภาพยนตร์อเมริกัน (MPAA)
กฎหมาย HIPAA ของสหรัฐอเมริกา	วัตถุประสงค์ประการหนึ่งของกฎหมาย HIPAA ของสหรัฐอเมริกาคือการส่งเสริมการใช้บันทึกสุขภาพอิเล็กทรอนิกส์ โดยเพิ่มประสิทธิภาพและคุณภาพของระบบการดูแลสุขภาพผ่านการแบ่งปันข้อมูลที่เข้มแข็ง HIPAA ให้มีความสำคัญและรับประกันความปลอดภัย (รวมถึงความพร้อมใช้งาน ความสมบูรณ์ และความเป็นส่วนตัว) และความเป็นส่วนตัวของข้อมูลสุขภาพที่ได้รับการปกป้อง (Protected Health Information: PHI) ระหว่างการสร้าง การรับ การบำรุงรักษา และการส่ง หน่วยงานที่อยู่ภายใต้การกำกับดูแลของ HIPAA และพันธมิตรทางธุรกิจของพวกเขาจำเป็นต้องจัดเตรียมมาตรการรักษาความปลอดภัยที่สอดคล้องกันในสถานการณ์ต่างๆ เช่น การประมวลผล การบำรุงรักษา และการจัดเก็บ PHI Tencent Cloud ผ่านการประเมินตนเอง เพื่อให้มั่นใจว่าความสามารถในการปกป้องความปลอดภัยของข้อมูลส่วนบุคคลของผู้ใช้และประสิทธิภาพของมาตรการควบคุมของ Tencent Cloud เป็นไปตามข้อกำหนดการปฏิบัติตามข้อกำหนดของ HIPAA
กฎ SEC ข้อ 17a-4 ของสหรัฐอเมริกา	บริการจัดเก็บวัตถุ (Object Storage: COS) ของ Tencent Cloud ได้รับการรับรองจากบริษัทประเมินบุคคลที่สามที่เป็นอิสระซึ่งมีความเชี่ยวชาญในการจัดการบันทึกและการกำกับดูแลข้อมูล ตามข้อกำหนดทางเทคนิคของคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์สหรัฐอเมริกา (Securities and Exchange Commission: SEC) องค์การกำกับดูแลการปฏิบัติงานในอุตสาหกรรมทางการเงิน (Financial Industry Regulatory Authority: FINRA) และคณะกรรมการการซื้อขายล่วงหน้าสินค้าโภคภัณฑ์ (Commodity Futures Trading Commission: CFTC) การรับรองนี้เป็นหลักประกันสำหรับลูกค้าที่ดำเนินการในสภาพแวดล้อมที่มีกฎระเบียบเข้มงวด (เช่น อุตสาหกรรมบริการทางการเงิน) ถึงวิธีการเก็บรักษาที่ไม่สามารถเขียนทับหรือลบได้และคุณสมบัติการล็อกวัตถุของ Tencent COS ซึ่งแสดงให้เห็นถึงความมุ่งมั่นของ Tencent Cloud

	ในการจัดหาผลิตภัณฑ์คลาวด์ที่ปลอดภัยและเป็นไปตามมาตรฐานอุตสาหกรรมให้กับลูกค้า
FISC ของญี่ปุ่น	เพื่อยกระดับความปลอดภัยของสถาบันการเงิน "คู่มือความปลอดภัยระบบคอมพิวเตอร์สำหรับธนาคารและสถาบันการเงินที่เกี่ยวข้องของ FISC" ให้คำแนะนำที่มีประสิทธิภาพในการสร้างระบบสารสนเทศที่ปลอดภัยและรับประกันการทำงานของระบบสารสนเทศสำหรับธนาคารและสถาบันการเงินของญี่ปุ่น Tencent Cloud ได้ประเมินสถานะการควบคุมตามคู่มือนี้ เพื่อยืนยันว่ามาตรการที่เกี่ยวข้องของ Tencent Cloud เป็นไปตามข้อกำหนดของคู่มือความปลอดภัยระบบคอมพิวเตอร์สำหรับธนาคารและสถาบันการเงินที่เกี่ยวข้องของ FISC
BS 10012: 2017 ของสหราชอาณาจักร	BS 10012: 2017 ได้รับการเผยแพร่โดยสถาบันมาตรฐานอังกฤษ (British Standards Institution: BSI) มีวัตถุประสงค์เพื่อจัดเตรียมกรอบการปฏิบัติตามข้อกำหนดและแนวปฏิบัติที่ดีสำหรับการปกป้องความเป็นส่วนตัวส่วนบุคคลให้กับองค์กร ขึ้นอย่างสำคัญในการสร้างและบำรุงรักษาระบบการจัดการข้อมูลส่วนบุคคล (Personal Information Management System: PIMS) และรับประกันว่าองค์กรมีมาตรการควบคุมที่เพียงพอและเหมาะสมเพื่อปกป้องข้อมูลส่วนบุคคล ระบบนี้ได้รับการอัปเดตและแก้ไขเพื่อให้สอดคล้องกับกฎระเบียบทั่วไปว่าด้วยการคุ้มครองข้อมูล (General Data Protection Regulation: GDPR) Tencent Cloud ได้รับการรับรอง BS 10012: 2017 แล้ว ซึ่งสะท้อนให้เห็นว่าระบบการจัดการข้อมูลส่วนบุคคลของ Tencent Cloud เป็นไปตามข้อกำหนดของมาตรฐานสากลและแนวปฏิบัติที่ดีของอุตสาหกรรม ทำให้ลูกค้าสามารถปฏิบัติตามข้อกำหนดการปกป้องความเป็นส่วนตัวส่วนบุคคลของ GDPR ได้ดียิ่งขึ้น
CISPE ของสหภาพยุโรป	รหัสประพฤติ CISPE เป็นแนวทางเฉพาะอุตสาหกรรมระดับแพน-ยุโรปสำหรับผู้ให้บริการโครงสร้างพื้นฐานคลาวด์ตามข้อ 40 ของกฎระเบียบทั่วไปว่าด้วยการคุ้มครองข้อมูล (GDPR) ของสหภาพยุโรป ช่วยให้องค์กรทั่วยุโรปสามารถเร่งการพัฒนาบริการบนคลาวด์ที่สอดคล้องกับ GDPR สำหรับผู้บริโภค ธุรกิจ และสถาบันต่างๆ Tencent Cloud ได้รับการมอบ "สถานะผู้สมัคร" สำหรับรหัสประพฤติ CISPE ซึ่งหมายความว่า Tencent Cloud ได้ดำเนินการประเมินตนเองตามข้อกำหนดของรหัสประพฤติ CISPE เสร็จสิ้นแล้ว เพื่อพิสูจน์การปฏิบัติตามข้อกำหนดของ Tencent Cloud ในระดับระบบเอกสารและกระบวนการนำไปปฏิบัติ
การรับรอง NIST CSF	NIST CSF เป็นกรอบการทำงานที่มุ่งเน้นการใช้ปัจจัยขับเคลื่อนทางธุรกิจเพื่อขึ้นนำกิจกรรมความปลอดภัยทางไซเบอร์ และพิจารณาความเสี่ยงด้านความปลอดภัยทางไซเบอร์เป็นส่วนหนึ่งของกระบวนการจัดการความเสี่ยงขององค์กร ช่วยให้องค์กรปรับปรุงกิจกรรมความปลอดภัยทางไซเบอร์และกำหนดลำดับความสำคัญตามความต้องการทางธุรกิจ ความสามารถในการทนต่อความเสี่ยง และทรัพยากรของตน และองค์กรสามารถเพิ่มความปลอดภัยและความยืดหยุ่นได้โดยการประยุกต์ใช้หลักการและแนวทางการจัดการความเสี่ยงของกรอบการทำงานนี้ Tencent Cloud ได้รับการรับรอง NIST CSF จากสถาบันบุคคลที่สามแล้ว ซึ่งไม่เพียงแต่เป็นการยืนยันความสามารถของระบบป้องกันความปลอดภัยทางไซเบอร์ของ

	Tencent Cloud เท่านั้น แต่ยังคงแสดงให้เห็นว่า Tencent Cloud สามารถระบุ ด้านทาน ตอบสนอง และจัดการกับความเสี่ยงด้านความปลอดภัยได้อย่างมีประสิทธิภาพ ปกป้องสินทรัพย์และข้อมูลบนคลาวด์ของลูกค้า และเสริมสร้างความมั่นใจของลูกค้าในความปลอดภัยและความเสถียรของ Tencent Cloud
การรับรอง PCI DSS	มาตรฐานความปลอดภัยข้อมูลสำหรับอุตสาหกรรมการเงินด้วยบัตร (Payment Card Industry Data Security Standard: PCI DSS) ได้รับการสร้างและบำรุงรักษาโดยคณะกรรมการมาตรฐานความปลอดภัยสำหรับอุตสาหกรรม การเงินด้วยบัตร (PCI Security Standards Council: PCI SSC) เพื่อเพิ่มความปลอดภัยของข้อมูลของผู้ถือบัตร PCI DSS จัดเตรียมเกณฑ์มาตรฐานระดับโลกสำหรับข้อกำหนดด้านเทคนิคและการดำเนินงานในการ ปกป้องข้อมูลบัญชี ซึ่งใช้กับหน่วยงานทั้งหมดที่เกี่ยวข้องกับการประมวลผลบัตรชำระเงิน เช่น ผู้ค้า ผู้ประมวลผล ผู้รับชำระเงิน ผู้ถือบัตร และผู้ให้บริการ รวมถึงหน่วยงานอื่นๆ ที่จัดเก็บ ประมวลผล หรือส่งข้อมูลของผู้ถือบัตร Tencent Cloud ผ่านการตรวจสอบการรับรอง PCI DSS แล้ว และได้รับคุณสมบัติผู้ให้บริการระดับ 1 ของ PCI DSS ซึ่งพิสูจน์ว่า Tencent Cloud สามารถให้บริการการเงินที่ปลอดภัยและน่าเชื่อถือแก่ลูกค้า และปกป้องความปลอดภัยของข้อมูลของผู้ถือบัตร
การปฏิบัติตาม ข้อกำหนด GxP	ในอุตสาหกรรมการดูแลสุขภาพ GxP ครอบคลุมกิจกรรมที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดที่กว้างขวาง โดยทั่วไปหมายถึงชุดของกฎระเบียบ แนวทาง หรือแนวปฏิบัติที่ดีของอุตสาหกรรมที่ควบคุมการพัฒนา การผลิต และการขายผลิตภัณฑ์ทางการแพทย์ เช่น ยา อุปกรณ์ทางการแพทย์ และแอปพลิเคชันซอฟต์แวร์ทางการแพทย์ Tencent Cloud ได้เผยแพร่หนังสือปกขาวเกี่ยวกับการปฏิบัติตามข้อกำหนด GxP เพื่ออธิบายให้ลูกค้าในอุตสาหกรรมการแพทย์ทราบว่ากระบวนการจัดการและมาตรการทาง เทคนิคของ Tencent Cloud สามารถช่วยลูกค้าให้เป็นไปตามข้อกำหนดของระบบคอมพิวเตอร์ GxP และรับประกันความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลธุรกิจของลูกค้าที่โฮสต์บน Tencent Cloud

03

โมเดลการแบ่งปันความ รับผิดชอบด้านความปล อดภัยของ Tencent Cloud

ในปัจจุบัน มีลูกค้ามากขึ้นเรื่อยๆ ที่คำนึงถึงความปลอดภัยเป็นปัจจัยสำคัญลำดับต้นๆ ในการเลือกผู้ให้บริการคอมพิวเตอร์คลาวด์และผลิตภัณฑ์และบริการที่พวกเขาให้มา Tencent Cloud ยึดถือคุณลักษณะของความปลอดภัยและการแบ่งปันของบริการคอมพิวเตอร์คลาวด์ เพิ่มความสามารถด้านความปลอดภัยของแพลตฟอร์มคลาวด์และบริการคลาวด์อย่างต่อเนื่อง และร่วมกับลูกค้าสร้างระบบการรับประกันความปลอดภัยที่ดีขึ้นและสมบูรณ์ยิ่งขึ้นสำหรับธุรกิจและข้อมูลบนคลาวด์ ในฐานะผู้ให้บริการคลาวด์ Tencent Cloud รับผิดชอบด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลและความปลอดภัยของแพลตฟอร์มคลาวด์ โดยคำนึงถึงว่าเมื่อลูกค้าเลือกประเภทบริการคลาวด์ที่แตกต่างกัน (เช่น บริการ IaaS, PaaS และ SaaS) สิทธิในการควบคุมส่วนประกอบต่างๆ จะแตกต่างกันไป ดังนั้น Tencent Cloud จึงสร้างโมเดลการแบ่งปันความรับผิดชอบด้านความปลอดภัยบนคลาวด์ตามประเภทบริการคลาวด์ที่แตกต่างกัน โดยส่วนที่มีสีฟ้าอ่อนถูกกำหนดให้เป็นความรับผิดชอบของ Tencent Cloud ส่วนที่มีสีเทาอ่อนเป็นความรับผิดชอบของลูกค้า และส่วนที่มีสีเขียวอ่อนแสดงว่า Tencent Cloud และลูกค้าจะแบ่งปันความรับผิดชอบร่วมกัน

	IaaS	PaaS	SaaS	
ความรับผิดชอบของลูกค้า	ความปลอดภัยของข้อมูลลูกค้าคลาวด์	ความปลอดภัยของข้อมูลลูกค้าคลาวด์	ความปลอดภัยของข้อมูลลูกค้าคลาวด์	
	กลยุทธ์บัญชีและการควบคุมการเข้าถึงของลูกค้าคลาวด์	กลยุทธ์บัญชีและการควบคุมการเข้าถึงของลูกค้าคลาวด์	กลยุทธ์บัญชีและการควบคุมการเข้าถึงของลูกค้าคลาวด์	
	กลยุทธ์การกำหนดค่าความปลอดภัยบนคลาวด์	กลยุทธ์การกำหนดค่าความปลอดภัยบนคลาวด์	กลยุทธ์การกำหนดค่าความปลอดภัยบนคลาวด์	ความรับผิดชอบร่วมกันในการกำหนดค่า
	ความปลอดภัยของแอปพลิเคชันบนคลาวด์	ความปลอดภัยของแอปพลิเคชันบนคลาวด์	ความปลอดภัยของแอปพลิเคชันบนคลาวด์	
	ความปลอดภัยของเครือข่ายเสมือนและโฮสต์บนคลาวด์	ความปลอดภัยของเครือข่ายเสมือนและโฮสต์บนคลาวด์	ความปลอดภัยของเครือข่ายเสมือนและโฮสต์บนคลาวด์	
ความรับผิดชอบของ Tencent Cloud	ความปลอดภัยและการปฏิบัติตามข้อกำหนดของแพลตฟอร์มและผลิตภัณฑ์คลาวด์เอง	ความปลอดภัยและการปฏิบัติตามข้อกำหนดของแพลตฟอร์มและผลิตภัณฑ์คลาวด์เอง	ความปลอดภัยและการปฏิบัติตามข้อกำหนดของแพลตฟอร์มและผลิตภัณฑ์คลาวด์เอง	
	ความปลอดภัยทางกายภาพและโครงสร้างพื้นฐาน	ความปลอดภัยทางกายภาพและโครงสร้างพื้นฐาน	ความปลอดภัยทางกายภาพและโครงสร้างพื้นฐาน	

รูปที่ 1: โมเดลการแบ่งปันความรับผิดชอบด้านความปลอดภัยข้อมูลของ Tencent Cloud

Tencent Cloud อธิบายคุณลักษณะด้านความปลอดภัยต่างๆ ในรูปแบบดังนี้:

- ความปลอดภัยของข้อมูลลูกค้าคลาวด์:**
 หมายถึงการจัดการความปลอดภัยของข้อมูลธุรกิจของลูกค้าเองในสภาพแวดล้อมคอมพิวเตอร์คลาวด์ รวมถึงข้อมูลธุรกิจของลูกค้าที่อัปโหลด จัดเก็บ แจกจ่าย ประมวลผล และจัดการในรูปแบบอื่นๆ
- กลยุทธ์บัญชีและการควบคุมการเข้าถึงของลูกค้าคลาวด์:** หมายถึงข้อมูลบัญชี Tencent Cloud ที่ลูกค้าลงทะเบียน และการดำเนินการทั้งหมดที่ได้รับอนุญาตภายใต้บัญชีคลาวด์ รวมถึงข้อมูลบัญชี รหัสผ่าน กลยุทธ์การควบคุมการเข้าถึง ข้อมูลการตรวจสอบสิทธิ์ ฯลฯ
- กลยุทธ์การกำหนดค่าความปลอดภัยบนคลาวด์:**
 หมายถึงกลยุทธ์ผลิตภัณฑ์ความปลอดภัยและการกำหนดค่าความปลอดภัยที่สอดคล้องกับข้อกำหนด

นิตด้านความปลอดภัยของธุรกิจและสถานการณ์ต่างๆ เพื่อการพัฒนาและใช้งานผลิตภัณฑ์คลาวด์
(รวมถึงผลิตภัณฑ์ความปลอดภัย) อย่างถูกต้อง

- **ความปลอดภัยของแอปพลิเคชันบนคลาวด์:**

หมายถึงการจัดการความปลอดภัยของระบบแอปพลิเคชันที่เกี่ยวข้องกับธุรกิจในสภาพแวดล้อมคอมพิวเตอรืคลาวด์ ซึ่งรวมถึงการออกแบบ การพัฒนา การเผยแพร่ การปฏิบัติการและบำรุงรักษา การตรวจสอบการดำเนินงาน เป็นต้น ของแอปพลิเคชัน

- **ความปลอดภัยของเครือข่ายเสมือนและโฮสต์บนคลาวด์:**

หมายถึงการจัดการความปลอดภัยของโฮสต์และเครือข่ายในสภาพแวดล้อมคอมพิวเตอรืคลาวด์ โดยในระดับเครือข่ายครอบคลุมเครือข่ายเสมือน ตัวปรับสมดุลโหลด เกตเวย์ความปลอดภัย VPN เส้นทางเชื่อมต่อเฉพาะทาง ฯลฯ ในระดับโฮสต์ครอบคลุมการจัดการระดับพื้นฐาน (เช่น ขั้นตอนควบคุมการทำให้เป็นเสมือน ระบบจัดการฐานข้อมูล เครือข่ายอาร์เรย์ดิสก์ ฯลฯ) และการจัดการการใช้งาน (เช่น โฮสต์เสมือน อีเมล CDN ระบบไฟล์ ฯลฯ) ของผลิตภัณฑ์คลาวด์ เช่น คอมพิวเตอรืคลาวด์ ที่เก็บข้อมูลคลาวด์ ฐานข้อมูลคลาวด์

- **ความปลอดภัยและการปฏิบัติตามข้อกำหนดของแพลตฟอร์มและผลิตภัณฑ์คลาวด์เอง:**

หมายถึงความปลอดภัยและการปฏิบัติตามข้อกำหนดของแพลตฟอร์มคลาวด์และผลิตภัณฑ์/บริการคลาวด์ที่ให้มาในสภาพแวดล้อมคอมพิวเตอรืคลาวด์

- **ความปลอดภัยทางกายภาพและโครงสร้างพื้นฐาน:**

หมายถึงการดำเนินงานด้านความปลอดภัยของศูนย์ข้อมูลและการจัดการความปลอดภัยของเซิร์ฟเวอร์และอุปกรณ์เครือข่ายกายภาพในสภาพแวดล้อมคอมพิวเตอรืคลาวด์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโมเดลการแบ่งปันความรับผิดชอบด้านความปลอดภัย โปรดอ้างอิง

[Tencent Cloud Security White Paper](#)

04

โครงสร้างพื้นฐานระดับ โลกของ Tencent Cloud

Tencent Cloud ได้จัดวางศูนย์ข้อมูลหลายแห่งทั่วโลก

ก่อให้เกิดเครือข่ายโครงสร้างพื้นฐานขนาดใหญ่ที่สามารถให้บริการที่รวดเร็ว เสถียร อัจฉริยะ และน่าเชื่อถือแก่ลูกค้าทั่วโลกด้วยระยะใกล้ Tencent Cloud ได้เปิดภูมิภาค (Region) มากกว่า 20 แห่งและดำเนินการโซนความพร้อมใช้งาน (Availability Zone) มากกว่า 60 แห่งในจีนแผ่นดินใหญ่ ภูมิภาคเอเชียแปซิฟิก ภูมิภาคอเมริกาเหนือ และภูมิภาคยุโรป

เพื่อมอบการสนับสนุนทางเทคนิคที่แข็งแกร่งให้กับธุรกิจจำนวนมากขึ้น

ช่วยให้ธุรกิจขยายตัวอย่างรวดเร็ว ช่วยลูกค้าเผชิญกับข้อกำหนดทางกฎระเบียบในภูมิภาคต่างๆ อย่างยืดหยุ่น

ตอบสนองความต้องการในการจัดเก็บข้อมูลในพื้นที่และโลกาภิวัตน์ทางธุรกิจขององค์กรในอุตสาหกรรม การเงิน และรับประกันความสอดคล้องตามกฎหมาย ความปลอดภัย

และประสิทธิภาพของการประมวลผลข้อมูล

- **ภูมิภาค (Region)** หมายถึงพื้นที่ทางภูมิศาสตร์ของศูนย์ข้อมูลทางกายภาพ ภูมิภาคต่างๆ ของ Tencent Cloud แยกจากกันโดยสมบูรณ์ เพื่อรับประกันความเสถียรและความทนทานต่อข้อผิดพลาดสูงสุดระหว่างภูมิภาคต่างๆ เพื่อลดความล่าช้าในการเข้าถึงและเพิ่มความเร็วในการดาวน์โหลด ขอแนะนำให้ลูกค้าเลือกภูมิภาคที่อยู่ใกล้ที่สุด
- **โซนความพร้อมใช้งาน (Availability Zone)** หมายถึงศูนย์ข้อมูลทางกายภาพของ Tencent Cloud ที่มีแหล่งจ่ายไฟและเครือข่ายอิสระจากกันภายในภูมิภาคเดียวกัน เป้าหมายคือเพื่อรับประกันว่าความล้มเหลวระหว่างโซนความพร้อมใช้งานจะถูกแยกจากกัน (ยกเว้นภัยพิบัติใหญ่หรือความล้มเหลวด้านไฟฟ้าขนาดใหญ่) ป้องกันไม่ให้ความล้มเหลวแพร่กระจาย และทำให้บริการทางธุรกิจของผู้ใช้สามารถให้บริการได้อย่างต่อเนื่อง โดยการเปิดอินสแตนซ์ภายในโซนความพร้อมใช้งานที่เป็นอิสระ ผู้ใช้สามารถปกป้องแอปพลิเคชันของตนจากผลกระทบของความล้มเหลวในตำแหน่งเดียว

ปัจจุบัน Tencent Cloud ได้ปรับใช้โหนดเร่งความเร็วมากกว่า 2,300 โหนดในประเทศจีน ครอบคลุมผู้ให้บริการหลายราย และได้จัดวางโหนดเร่งความเร็วมากกว่า 900 โหนดนอกประเทศจีน ครอบคลุมกว่า 70 ประเทศและภูมิภาคทั่วโลก

โดยการกระจายเนื้อหาบริการไปยังโหนดเร่งความเร็วทั่วเครือข่าย

และใช้ระบบจัดตารางทั่วโลกเพื่อให้ผู้ใช้สามารถรับเนื้อหาที่ต้องการจากโหนดใกล้เคียงได้ ลดความล่าช้าในการเข้าถึง

Tencent Cloud ยังได้สร้างไซโตอิสระ และใช้วิธีการทางเทคนิค เช่น การเข้ารหัสข้อมูล การควบคุมการเข้าถึง การติดตามการตรวจสอบ เป็นต้น เพื่อเพิ่มการแยกข้อมูลและความปลอดภัย ป้องกันการรั่วไหลของข้อมูลและการเข้าถึงที่ผิดกฎหมาย และเสริมสร้างการแยกข้อมูลตามภูมิภาคและการประมวลผลที่สอดคล้องตามกฎหมาย

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโครงสร้างพื้นฐานของ Tencent Cloud โปรดดูที่หน้า [Tencent Cloud Global Infrastructure](#).

05

Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ
หลักเกณฑ์การกำกับดูแลความ
เสี่ยงด้านเทคโนโลยีสารสนเทศ
ของสถาบันการเงินและสถาบัน
การเงินเฉพาะกิจ ของ BOT
อย่างไร

เพื่อปรับตัวให้สอดคล้องกับสภาพแวดล้อมความเสี่ยงและรูปแบบธุรกิจที่เปลี่ยนแปลงอย่างต่อเนื่อง ตลอดจนเพิ่มความยืดหยุ่น ประสิทธิภาพ และความชัดเจนของกฎระเบียบ ธนาคารแห่งประเทศไทย (BOT) ได้จัดทำและเผยแพร่ [BOT No. Sor Gor Chor 5/2566 เรื่อง](#)

[หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ \(Information Technology risk\) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ](#) ในปี 2566

กฎระเบียบใหม่นี้ได้รวมสถาบันการเงินเฉพาะทาง เช่น ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร และธนาคารออมสิน เข้าสู่ขอบเขตการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นครั้งแรก ซึ่งทำให้เกิดการกำกับดูแลแบบรวมสำหรับ สถาบันการเงิน¹ และ สถาบันการเงินเฉพาะทาง²

กฎระเบียบใหม่นี้มีศูนย์กลางอยู่ที่การกำกับดูแลเทคโนโลยีสารสนเทศ

การจัดการความปลอดภัยเทคโนโลยีสารสนเทศ การจัดการความเสี่ยงเทคโนโลยีสารสนเทศ

การปฏิบัติตามเทคโนโลยีสารสนเทศ และการตรวจสอบเทคโนโลยีสารสนเทศ

โดยมีภาคผนวกแยกต่างหากสำหรับแต่ละด้าน เพื่อให้คำแนะนำในการดำเนินงานที่ละเอียดยิ่งขึ้น

ในบทนี้ Tencent Cloud จะสรุปและเรียบเรียงข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จาก หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ของ BOT และอธิบายว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud

จะช่วยสถาบันการเงินและสถาบันการเงินเฉพาะทางในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

นอกจากนี้ ธนาคารแห่งประเทศไทยยังได้อัปเดตและเผยแพร่ภาคผนวก

"แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ" และ

"แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก" พร้อมกัน:

- ภาคผนวก "แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ" มีความสอดคล้องอย่างสูงกับเนื้อหาหลักของภาคผนวกแต่ละด้านในกฎระเบียบใหม่ ในฐานะผู้ให้บริการคลาวด์ วิธีการที่ Tencent Cloud ปฏิบัติตามและช่วยเหลือลูกค้าให้เป็นไปตามข้อกำหนดที่เกี่ยวข้องของภาคผนวกนี้ สถาบันการเงินและสถาบันการเงินเฉพาะทางสามารถอ้างอิงเนื้อหาที่สอดคล้องกันในบทที่ 5.2-5.6 ของเอกสารนี้
- ภาคผนวก "แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก" ให้กรอบคำแนะนำแก่สถาบันการเงินและสถาบันการเงินเฉพาะทาง เพื่อให้สามารถใช้มาตรการจัดการความเสี่ยงที่เกี่ยวข้องอย่างสมเหตุสมผลและเหมาะสมตามขอบเขตการใช้บริการภายนอก วิธีการเชื่อมต่อ สิทธิการเข้าถึงข้อมูล ระดับความเสี่ยงและความสำคัญ สำหรับกรณีที่ให้บริการคอมพิวเตอร์คลาวด์เพื่อสนับสนุนระบบที่สำคัญ สถาบันการเงินและสถาบันการเงินเฉพาะทางต้องปฏิบัติตามข้อกำหนดทั้งหมดในส่วนที่สามของแนวทางนี้โดยสมบูรณ์ ดังนั้น ในบทที่ 5.7 Tencent Cloud จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จาก "

¹ "สถาบันการเงิน" หมายความว่าสถาบันการเงินตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

² "สถาบันการเงินเฉพาะทาง" หมายถึงสถาบันการเงินเฉพาะทางที่จัดตั้งขึ้นตามกฎหมายเฉพาะ

โดยมีวัตถุประสงค์เพื่อสนับสนุนนโยบายของรัฐบาลในการส่งเสริมการพัฒนาเศรษฐกิจและสนับสนุนการลงทุน ได้แก่ ธนาคารออมสิน ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร ธนาคารอาคารสงเคราะห์ ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย ธนาคารอิสลามแห่งประเทศไทย และบริษัท หลักทรัพย์ไทยเครดิต ประกันภัย จำกัด (มหาชน)

แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก"
และอธิบายว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud
จะช่วยสถาบันการเงินและสถาบันการเงินเฉพาะทางในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

5.1 หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ-เนื้อหาหลัก

5.1.1 หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการค วบคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
7.1	ธรรมาภิบาลด้าน เทคโนโลยีสาร สนเทศ	จัดให้มีโครงสร้างและบทบาทหน้าที่คว ามรับผิดชอบในการกำกับดูแลความ เสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเห มาะสมตั้งแต่คณะกรรมการของสถาบั นการเงินหรือคณะกรรมการของสถา บันการเงินเฉพาะกิจและผู้บริหารระดับ สูงที่มีความสำคัญในการผลักดันและ ยกระดับการบริหารความเสี่ยงด้านเทค โนโลยีสารสนเทศกำหนดให้มีนโยบาย ที่เกี่ยวข้องกับการกำกับดูแลความเสี ย ด้านเทคโนโลยีสารสนเทศ อสารและกำกับดูแลให้มีการปฏิบัติตาม นโยบายที่กำหนด นอกจากนี้ ต้องจัดให้มีผู้รับผิดชอบในการบริหารจั ดการความมั่นคงปลอดภัยด้านเทคโน โลยีสารสนเทศ รวมทั้ง สร้างวัฒนธรรมและพฤติกรรมร่วมขอ งทุกคนในองค์กรให้ตระหนักถึงความ เสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อ เนื่อง (รายละเอียดในเอกสารแนบ 1)	ลูกค้าควรสร้างโครงสร้างการกำกับดูแลความเสี่ยงด้ านเทคโนโลยีสารสนเทศที่แข็งแกร่งและความรับผิดชอบ ของคณะกรรมการและผู้บริหารระดับสูงและกำหนด นโยบายการกำกับดูแลความเสี่ยงด้านเทคโนโลยี สารสนเทศโดยฝ่ายบริหารควรกำกับดูแลการดำเนินก ารตามนโยบายดังกล่าว นอกจากนี้ ลูกค้ายังควรแต่งตั้งบุคคลเฉพาะรับผิดชอบด้านกาจั ดการความปลอดภัยเทคโนโลยีสารสนเทศและสร้างวั ฒนธรรมการตระหนักรู้เกี่ยวกับความเสี่ยงด้านเทคโน โลยีสารสนเทศภายในองค์กร เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการ กำกับดูแล ในด้านกลยุทธ์ความปลอดภัยทางไซเบอร์ เพื่อรับมือกับภัยคุกคามทางเครือข่ายและความเสี่ยง ด้านความปลอดภัยที่ซับซ้อนมากขึ้นในยุคดิจิทัล Tencent Cloud ได้เปิดตัวกรอบแบบจำลอง "ภูมิคุ้มกันปลอดภัยดิจิทัล" เสนอให้ใช้แนวคิดด้านภูมิคุ้มกันในการรับมือกับควา มสัมพันธ์เชิงประสานงานระหว่างการสร้างความปลอ ดภัยและการพัฒนาธุรกิจในยุคใหม่ โดยกำหนดเป้าหมายที่ข้อมูลและธุรกิจขององค์กร เพื่อสร้างระบบภูมิคุ้มกันความปลอดภัยที่มีความยืด หยุ่น ปรับตัวได้ และขยายได้ ช่วยคุ้มครองการพัฒนาคุณภาพสูงขององค์กรในยุค ดิจิทัล Tencent Cloud มีเป้าหมาย "เสริมสร้างภูมิคุ้มกันปลอดภัยดิจิทัลขององค์กร สนับสนุนการพัฒนาที่มีความยืดหยุ่นในยุคดิจิทัล" มุ่งมั่นปรับปรุงระบบความปลอดภัยบนคลาวด์ของตน เองสร้างขีดความสามารถด้านความปลอดภัยและกา รปฏิบัติตามข้อกำหนด และกำหนดมาตรฐานความปลอดภัยบนคลาวด์ โดยอิงตามกรอบแบบจำลองที่วางแผนอย่างครอบคลุม

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ผ่านผลิตภัณฑ์ที่หลากหลายและคุณลักษณะด้านคว ามปลอดภัย Tencent Cloud บรรลุการป้องกันในทุกด้าน และนำฟังก์ชันความปลอดภัยที่สอดคล้องกันไปใช้ใน ผลิตภัณฑ์ทุกระดับ Tencent Cloud ได้จัดตั้งคณะกรรมการเทคโนโลยีความปลอดภัยและ ทีมงานความปลอดภัยมืออาชีพที่มีหน้าที่และสาขาวิ ชาที่แตกต่างกัน และได้สร้างมาตรฐานและขั้นตอนการจัดการทรัพยากร บุคคลที่สมบูรณภายในองค์กร เพื่อให้มั่นใจในการคัดเลือก จ้าง และจัดวางบุคลากรตามข้อกำหนดของตำแหน่งงาน Tencent Cloud รวบรวมทีมบริการผู้เชี่ยวชาญที่มีประสบการณ์ในอุต สาหกรรม มุ่งมั่นให้บริการผลิตภัณฑ์และบริการที่ปลอดภัย น่าเชื่อถือ เป็นมืออาชีพ และเป็นไปตามข้อกำหนดแก่ลูกค้า สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำกับดูแลเทคโนโลยี สารสนเทศ โปรดดูบทที่ 5.2 "5.2 เอกสารแนบ 1 ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศของสถาบันก ารเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
7.2	การบริหรจัดก ารความมั่นคงป ลอดภัยด้านเทค โนโลยีสารสนเทศ	จัดให้มีการบริหารจัดการและควบคุมร บบเทคโนโลยีสารสนเทศที่รองรับการใ ้บริการ ให้มีการรักษาความลับของระบบและช้ ้อมูล ถูกต้องเชื่อถือได้ ละพร้อมใช้งาน โดยน่านโยบาย การรักษาความมั่นคงปลอดภัยด้านเท คโนโลยีสารสนเทศมาจัดทำระเบียบวิธี ปฏิบัติและกระบวนการรักษา ความมั่นคงปลอดภัยด้านเทคโนโลยีสา รสนเทศของสถาบันการเงินและสถาบัน การเงินเฉพาะกิจ(รายละเอียดในเอก สารแนบ 2)	ลูกค้าควรกำหนดและบำรุงรักษานโยบาย มาตรฐาน และขั้นตอนด้านความปลอดภัยทางเทคโนโลยี เพื่อบริหารจัดการและควบคุมระบบเทคโนโลยีสารสนเทศที่สนับสนุนการดำเนินงานของบริการ และควรทบทวนและปรับปรุงนโยบายและกระบวนการ เหล่านี้เป็นประจำ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการ กำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูล ซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยช้ ้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดก ารความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ รวมถึงชี้้นำการทำงานประจำวันและกระบวนการจัดก ารของหน่วยงานและพนักงานทุกหน่วยในบริษัท

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			นโยบายความปลอดภัยข้อมูลของ Tencent Cloud จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัยบนคลาวด์สอดคล้องกับนโยบายความปลอดภัยมาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบายความปลอดภัยข้อมูล สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการความปลอดภัยเทคโนโลยีสารสนเทศ โปรดดูบทที่ 5.3 "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
7.3	การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	จัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างครอบคลุมทั่วทั้งองค์กร โดยประสานงานร่วมกับหน่วยงานธุรกิจและหน่วยงานด้านเทคโนโลยีสารสนเทศ ในการระบุและประเมิน ความเสี่ยง การกำหนดมาตรการในการลดความเสี่ยงและระบบการควบคุมภายใน เพื่อให้มั่นใจว่า มีการบริหารความเสี่ยงอย่างเหมาะสม สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ (รายละเอียดใน เอกสารแนบ 3)	ลูกค้าควรกำหนดระบบการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดำเนินการปฏิบัติการจัดการความเสี่ยงและมาตรการควบคุมที่มีประสิทธิภาพ ชี้แจงผู้รับผิดชอบที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และทบทวนนโยบายการจัดการความเสี่ยงเป็นประจำ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดการกำกับดูแล Tencent Cloud ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามงานต่างๆ เช่น การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยงไว้อย่างชัดเจน Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุความเสี่ยงตามสถานการณ์ความเสี่ยง ผลกระทบทางธุรกิจ หรือกระบวนการให้บริการ สำหรับความเสี่ยงที่ระบุได้ Tencent Cloud จะประเมินความเป็นไปได้และระดับผลกระทบของความเสี่ยงแต่ละรายการเพื่อจำแนกระดับความเสี่ยง และดำเนินการตามขั้นตอนที่สอดคล้องกันต่อไป โดยมีการบันทึกกิจกรรมกระบวนการทั้งหมดไว้

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Tencent Cloud ยังติดตามสถานการณ์การจัดการความเสี่ยงอย่างต่อเนื่อง ประเมินความเสี่ยงที่เหลืออยู่ และให้มั่นใจว่าผู้เกี่ยวข้องได้จัดการความเสี่ยงอย่างเหมาะสมตามข้อกำหนดการจัดการความเสี่ยงของ Tencent Cloud นอกจากนี้ Tencent Cloud บำรุงรักษาและปรับปรุงวิธีการประเมินความเสี่ยงและทะเบียนความเสี่ยงอย่างต่อเนื่องตามแนวโน้มการเปลี่ยนแปลงในอุตสาหกรรมคลาวด์และแนวปฏิบัติการจัดการภายใน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โปรดดูบทที่ 5.4 "5.4 เอกสารแนบ 3 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
7.4	การปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	จัดให้มีการติดตามดูแลและสอบทานการปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ เพื่อป้องกัน การฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและกฎเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง (รายละเอียดในเอกสารแนบ4)	ลูกค้าควรกำกับดูแลการปฏิบัติตามกฎหมายระเบียบข้อบังคับ และข้อกำหนดทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศของตน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด และได้สร้างขั้นตอนที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านความปลอดภัย เพื่อให้มั่นใจว่าการดำเนินการด้านความปลอดภัยข้อมูลเป็นไปตามข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ มาตรฐาน และขั้นตอนที่เกี่ยวข้อง ทีมงานฝ่ายกฎหมายของ Tencent Cloud จะระบุและรวบรวมข้อกำหนดการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับธุรกิจของ Tencent Cloud อย่างต่อเนื่อง จัดทำเป็นรายการกฎหมายและระเบียบข้อบังคับที่สอดคล้องกัน และบำรุงรักษาและปรับปรุงเป็นประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศ โปรดดูบทที่ 5.5 "5.5 เอกสารแนบ 4 การกำกับปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ"

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			<u>ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ"</u> ในคู่มือนี้
7.5	การตรวจสอบด้ านเทคโนโลยีสา รสนเทศ	จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำเร็จและความเสี่ยงจากการใช้งานเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบที่มีความเป็นอิสระ รวมทั้งต้องติดตามให้มีการปรับปรุงแก้ไขประเด็นจากการตรวจสอบ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยงและการปฏิบัติตามกฎหมายที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศอย่างเพียงพอ เหมาะสม (รายละเอียดในเอกสารแนบ 5)	ลูกค้าควรสร้างกลไกการตรวจสอบเทคโนโลยีสารสนเทศ ดำเนินการตรวจสอบความเสี่ยงทางเทคนิคเป็นประจำ และติดตามการดำเนินการแก้ไขปัญหาที่พบในการตรวจสอบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยภายในอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบการจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็นอิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริกาการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจาก "Compliance Document Download"

ลำดับ ที่	โดเมนการค วบรวม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบเทคโนโลยีสารสนเทศ โปรดดูที่ 5.6 " 5.6 เอกสารแนบ 5 การตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ " ในคู่มือนี้

5.1.2 การแจ้งการรายงาน หรือการขออนุญาต ต่ออปท

ลำดับ ที่	โดเมนการค วบรวม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
10.1	การแจ้งหรือการ ขออนุญาตนำเท คโนโลยีสารส นเทศมาใช้หรือ การเปลี่ยนแปลง ง ระบบหรือเทคโนโลยีสารสนเทศ ที่มีนัยสำคัญ	10.1.1 ธนาคารพาณิชย์ที่นำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบ หรือเทคโนโลยีสารสนเทศ โดยการนำมาใช้หรือการเปลี่ยนแปลง ดังกล่าวมีนัยสำคัญตามข้อกำหนด ที่ธนาคารพาณิชย์ได้กำหนดขึ้นตาม ข้อ 9 ทั้งกรณีที่ธนาคารพาณิชย์ดำเนินการ เองและกรณีที่มีการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกต้องแจ้งการนำมาใช้หรือการเปลี่ยนแปลงดังกล่าว ต่อ อปท. ตามที่กำหนดในคู่มือสำหรับประชาชน ล่วงหน้าไม่น้อยกว่า 15 วัน ก่อนดำเนินการ เว้นแต่ อปท. มีคำสั่งให้ธนาคารพาณิชย์ไม่ต้องแจ้ง การนำเทคโนโลยีสารสนเทศมาใช้ หรือเปลี่ยนแปลงระบบ หรือเทคโนโลยีสารสนเทศที่มีนัยสำคัญ 10.1.2 สถาบันการเงินเฉพาะกิจ บริษัทเงินทุน บริษัทเครดิตฟองซิเอร์ที่นำเทคโนโลยี สารสนเทศมาใช้หรือเปลี่ยนแปลงระบบ หรือเทคโนโลยีสารสนเทศ โดยการนำมาใช้หรือการเปลี่ยนแปลง ดังกล่าวมีนัยสำคัญตามข้อกำหนดตาม ข้อ 9 ทั้งกรณีที่ทำดำเนินการเองและกรณีที่มีการ ใช้บริการ การเชื่อมต่อ	ลูกค้าที่จะนำเทคโนโลยีสำคัญมาใช้หรือจะเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศครั้งใหญ่ ไม่ว่าการเปลี่ยนแปลงนั้นจะดำเนินการด้วยตนเองหรือ โดยผู้ให้บริการบุคคลที่สาม ต้องแจ้งผ่านช่องทางที่ธนาคารแห่งประเทศไทยกำหนด และได้รับอนุญาตล่วงหน้าไม่น้อยกว่า 15 วันก่อนการดำเนินการ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการ กำกับดูแล Tencent Cloud จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอ การดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน และขอบเขตของการเปลี่ยนแปลง สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแวดล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขยาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดความเฉพาะ	การตอบสนองของ Tencent Cloud
		หรือการเข้าถึงข้อมูลจากบุคคลภายนอกต้องยื่นขออนุญาตก่อนนำมาใช้หรือก่อนการเปลี่ยนแปลง ดังกล่าวต่ออปท. ตามที่กำหนดในคู่มือสำหรับประชาชน	
10.3	การรายงานปัญหาหรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องรายงานปัญหาหรือเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศต่ออปท. ตามรูปแบบและช่องทางที่กำหนดโดยเร็วเมื่อทราบถึง (1) เหตุการณ์ด้านเทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการทำงานของระบบงาน หรือชื่อเสียงที่มี นัยสำคัญและเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุด หรือ (2) กรณี เทคโนโลยีสารสนเทศที่มีนัยสำคัญถูกโจมตีหรือถูกขโมยข้อมูลจากภัยคุกคามทางไซเบอร์และ (3) กรณี ปัญหาหรือเหตุขัดข้องของระบบเทคโนโลยีสารสนเทศที่ส่งผลกระทบต่อให้บริการผ่านช่องทางให้บริการสำคัญที่ประชาชนใช้บริการจำนวนมากตามที่ อปท. กำหนด ทั้งนี้สามารถแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมในภายหลังได้	ลูกค้าที่เกิดหรือพบปัญหาหรือเหตุการณ์สำคัญด้านเทคโนโลยีสารสนเทศต้องแจ้งผ่านช่องทางที่ธนาคารแห่งประเทศไทยกำหนดทันที และภายหลังต้องชี้แจงเพิ่มเติมถึงสาเหตุของเหตุการณ์และมาตรการแก้ไข เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการสื่อสารและการแจ้งเหตุการณ์ Tencent Cloud ได้กำหนดมาตรฐานการจัดการเหตุการณ์ความปลอดภัยข้อมูล สร้างขั้นตอนที่เกี่ยวข้อง เช่น การตอบสนองเหตุการณ์ความปลอดภัยข้อมูล การยกระดับเหตุการณ์ และการแจ้งเหตุการณ์ เพื่อแจ้งเตือนหรือแจ้งให้พนักงานภายในบริษัท ลูกค้าและผู้เกี่ยวข้องอื่น ๆ ที่อาจหรือได้รับผลกระทบจากอุบัติเหตุทราบทันเวลา ทำให้ทุกฝ่ายสามารถสื่อสารและประสานงานกันอย่างมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้เหลือน้อยที่สุด ในด้านการที่ลูกค้าแจ้งปัญหาหรือติดต่อ Tencent Cloud คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการใช้งาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับ

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ระบบใบงานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับใบงานของลูกค้าผ่านกลไกการตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วม และจัดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้าได้รับการตอบสนองและจัดการอย่างทันท่วงที นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้าได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเวลา ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับการสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า
10.4	การรายงานข้อมูลต่อธนาคารแห่งประเทศไทย	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดทำและจัดส่งแบบรายงานในรูปแบบและตามระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนดรวมถึงจัดทำและจัดส่งรายงานและข้อมูลอื่นเพิ่มเติมเป็นรายกรณีตามที่ธนาคารแห่งประเทศไทยร้องขอ	ลูกค้าควรจัดทำและส่งรายงานตามเวลาที่ธนาคารแห่งประเทศไทยกำหนดไว้ในรูปแบบที่กำหนด และภายใน 30 วันนับจากสิ้นปีปฏิทินทุกปี ควรส่งรายงานประเมินการปฏิบัติตามข้อกำหนดการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามรูปแบบและช่องทางที่ธนาคารแห่งประเทศไทยกำหนด เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud
10.5	การรายงานผลการประเมินการปฏิบัติตามหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดส่งผลการประเมินการปฏิบัติตามหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ ธปท. ทราบภายใน 30 วัน นับแต่วันสิ้นปีปฏิทิน โดยมีรูปแบบและช่องทางตามที่ ธปท.	จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเทศไทย Tencent Cloud ยังได้รับการตรวจสอบโดยบุคคลที่สามอิสระมืออาชีพ

ลำดับ ที่	โดเมนการค วาคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		กำหนด	เป็นประจำ โดยผ่านการจัดทำรายการการควบคุมระบบและองค์ กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริ การล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคล ที่สามที่เป็นอิสระแล้ว Tencent Cloud จะจัดเตรียมสำเนารายงานการตรวจสอบตามความต้ องการจริงของลูกค้า

5.2 เอกสารแนบ 1

ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเ พาะกิจ

ลำดับที่	โดเมน	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ รูปแบบ 1	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องจัดให้มี (1) นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) และ (2) นโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management policy) โดยนโยบายดังกล่าวต้องได้รับการอนุมัติจากคณะกรรมการของสถาบันการเงินหรือคณะกรรมการของสถาบันการเงิน	ลูกค้าควรกำหนดนโยบายความปลอดภัยเทคโนโลยีสารสนเทศและนโยบายการจัดการความเสี่ยงให้สอดคล้องกับลักษณะ ขนาด และสถานะความเสี่ยงของธุรกิจ และควรทบทวนและปรับปรุงนโยบายเหล่านี้เป็นประจำ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางกำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูล ซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยข้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดการความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ
3.1, 3.2	1.3.1-1.3.5	นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ	

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดควบคุมเจ เพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
1	นโยบายสารสนเทศ		เฉพาะกิจ และต้องสอดคล้องกับกลยุทธ์ในการนำเทคโนโลยีสารสนเทศมาใช้สำหรับให้บริการหรือดำเนินธุรกิจ รวมทั้งสอดคล้องกับแนวทางการบริหารความเสี่ยงและการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากลหรือ มาตรฐานที่ได้รับการยอมรับโดยทั่วไป สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องทบทวนนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อย ปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ	รวมถึงชี้้นำการทำงานประจำวันและกระบวนการจัดการของหน่วยงานและพนักงานทุกหน่วยในบริษัท นโยบายความปลอดภัยข้อมูลของ Tencent Cloud จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัยบนคลาวด์สอดคล้องกับนโยบายความปลอดภัย มาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบายความปลอดภัยข้อมูล นอกจากนี้ Tencent Cloud ยังได้รับใบรับรองและคุณวุฒิด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดความเป็นส่วนตัวหลายรายการ เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, SOC ซึ่งพิสูจน์ว่าการจัดการความปลอดภัยและการสร้างการป้องกันข้อมูลส่วนบุคคลของ Tencent Cloud เป็นไปตามมาตรฐานการรับรองที่เกี่ยวข้องหรือแนวปฏิบัติที่ดีของอุตสาหกรรม และยังได้รับการตรวจสอบจากสถาบันตรวจสอบบุคคลที่สามมืออาชีพเป็นประจำอีกด้วย
4.1, 4.2, 4.3	1.4.1-1.4.6	การบริหารจัดการบุคลากร	การทำหน้าที่ปฏิบัติงาน บริหารความเสี่ยงและกำกับการ ปฏิบัติตามกฎหมาย และตรวจสอบที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ ต้องครอบคลุมในเรื่องกระบวนการ คัดเลือกบุคลากรที่มีความรู้หรือประสบการณ์เพียงพอในการปฏิบัติหน้าที่ ความเพียงพอของบุคลากรที่สอดคล้องกับปริมาณการใช้เทคโนโลยี	ลูกค้าควรจัดการบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเหมาะสม เช่น การสร้างกระบวนการคัดเลือกบุคลากร การลงนามในข้อตกลงรักษาความลับกับพนักงาน และกลไกการจัดการเมื่อพนักงานลาออกหรือเปลี่ยนตำแหน่ง เป็นต้น เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานและขั้นตอนการจัดการทรัพยากรบุคคลที่สมบูรณ์ เพื่อให้มั่นใจในการคัดเลือก จ้าง และจัดวางบุคลากรตามข้อกำหนดของตำแหน่งงาน ก่อนเข้าทำงาน

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดควบคุมเจ เพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริหาร			
รแบบ	ารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
1	นโลยสารสนเทศ		ยสารสนเทศ และมาตรการในการสร้างและส่งเสริมให้บุคลากรตระหนักถึง ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ข้อกำหนดหรือเงื่อนไขในสัญญาจ้างงานของบุคลากรหรือระเบียบข้อบังคับภายในองค์กร ควรระบุเรื่องความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างชัดเจนเพื่อป้องกันการรั่วไหลของข้อมูลหรือความเสียหายที่อาจเกิดขึ้น การบริหารจัดการสิทธิของบุคลากรที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ ต้องปรับปรุงให้เป็นปัจจุบันโดยเฉพาะเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน รวมทั้ง ต้องสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงการเปลี่ยนแปลงดังกล่าว	ผู้สมัครจะต้องผ่านการสัมภาษณ์ โดย Tencent Cloud จะประเมินว่าตนมีคุณสมบัติตรงตามความสามารถที่ตำแหน่งงานต้องการหรือไม่ ตามกฎหมายที่ใช้บังคับและระดับตำแหน่งงาน ฝ่ายทรัพยากรบุคคลจะทำการตรวจสอบประวัติของผู้สมัครก่อนการจ้างงาน การตรวจสอบประวัติรวมถึงประวัติการทำงานในอดีต การตรวจสอบประวัติอาชญากรรม และการตรวจสอบวุฒิการศึกษา ผลการตรวจสอบประวัติจะถูกบันทึกไว้ในระบบการจัดการทรัพยากรบุคคลของ Tencent Cloud หลังจากรับเข้าทำงาน พนักงานภายในทุกคนต้องลงนามในสัญญาจ้างและข้อตกลงรักษาความลับ โดยสัญญาจ้างได้ระบุกลยุทธ์ความปลอดภัยที่มีอยู่ของ Tencent Cloud รวมถึงความรับผิดชอบด้านความปลอดภัยข้อมูลและความรับผิดชอบในการปกป้องข้อมูลส่วนบุคคลที่พนักงานหรือบุคคลที่สามต้องปฏิบัติตาม ส่วนข้อตกลงรักษาความลับประกอบด้วยข้อผูกพันและความรับผิดชอบในการรักษาความลับของบุคคลที่ลงนาม และบทลงโทษที่อาจได้รับหากมีการละเมิดข้อกำหนดในการรักษาความลับ พนักงานภายนอก (Outsourcing) ก็จำเป็นต้องได้รับการตรวจสอบประวัติก่อนการจ้างงานเช่นเดียวกัน และต้องปฏิบัติตามข้อกำหนดในการรักษาความลับที่กำหนดไว้ในข้อตกลงระหว่าง Tencent Cloud กับผู้ให้บริการภายนอก ข้อกำหนดในการรักษาความลับระหว่าง Tencent Cloud กับพนักงานและบุคคลที่สามจะได้รับการทบทวนและปรับปรุงโดยฝ่ายกฎหมายตามความจำเป็น ในระหว่างการทำงานของพนักงานหรือบุคคลที่สาม Tencent Cloud ได้สร้างกลไกการฝึกอบรมและการเรียนรู้ด้านความปลอดภัยข้อมูลหลายชุด

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดควบคุมเจ เพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริหาร			
รแบบ	ารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
1	นโลยสารสนเทศ			เพื่อให้ความรู้แก่พนักงานเกี่ยวกับนโยบาย ขั้นตอน และแนวทางปฏิบัติด้านความปลอดภัยข้อมูล พนักงานต้องเข้ารับการฝึกอบรมสร้างจิตสำนึกด้านความปลอดภัยข้อมูลเป็นประจำ ขั้นตอนการลาออกจาก Tencent Cloud รวมถึงการยกเลิกบัญชีผู้ใช้และสิทธิ์การเข้าถึงทันที ตลอดจนกระบวนการเรียกคืนทรัพย์สินของบริษัท เป็นต้น ทรัพย์สินที่มีตัวตนของ Tencent Cloud ถูกจัดสรรให้กับผู้รับผิดชอบที่กำหนดและถูกบันทึกไว้ผ่านระบบติดตามทรัพย์สินเฉพาะภายในของ Tencent Cloud Tencent Cloud จะทำการตรวจนับทรัพย์สินเป็นประจำเพื่อยืนยันการมีอยู่จริงของทรัพย์สิน และบันทึกผลการตรวจนับ
5	1.5.1-1.5.3	การส่งเสริมให้บุคลากรตระหนักถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศ	สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องสื่อสารและให้ความรู้แก่บุคลากรที่ทำหน้าที่ปฏิบัติงาน บริหารความเสี่ยงและการปฏิบัติตามกฎเกณฑ์ และตรวจสอบที่เกี่ยวข้องกับ ด้านเทคโนโลยีสารสนเทศ รวมถึงบุคลากรที่ใช้เทคโนโลยีสารสนเทศปฏิบัติงานประจำวันอย่างเพียงพอ และเหมาะสม เพื่อให้บุคลากรเข้าใจและตระหนักถึงความสำคัญของความเสี่ยงด้านเทคโนโลยีสารสนเทศและ การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย เช่น การจัดอบรมให้ความรู้แก่บุคลากรเกี่ยวกับการใช้งาน อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับเครือข่ายสาธารณะ ที่ถูกต้อง	ลูกค้าควรจัดฝึกอบรมการรับรู้ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้กับบุคลากรที่เกี่ยวข้อง และสื่อสารความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์แก่ลูกค้าและผู้ให้บริการอย่างต่อเนื่องและเชิงรุก เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดมาตรฐานการจัดการความปลอดภัยทรัพยากรบุคคลที่สมบูรณ์ภายในองค์กร ซึ่งรวมถึงการตรวจสอบความสามารถและคุณวุฒิ ก่อนเข้าทำงานของพนักงาน และการฝึกอบรมทักษะตามตำแหน่งหลังเข้าทำงาน เป็นต้น Tencent Cloud ยังได้สร้างกลไกการฝึกอบรมความปลอดภัยข้อมูลที่สมบูรณ์ภายในองค์กร โดยกำหนดให้พนักงานประจำ ที่ปรึกษา นักฝึกงาน และพนักงานภายนอก ต้องเรียนหลักสูตรฝึกอบรมความปลอดภัยข้อมูล หลักสูตรฝึกอบรมที่เกี่ยวข้องประกอบด้วยการฝึกอบรมบังคับสำหรับพนักงานทุกคน การฝึกอบรมเฉพาะทางสำหรับตำแหน่งงานสำคัญ และการฝึกอบรมวิชาชีพเลือกได้เอง เป็นต้น โดยเนื้อหาครอบคลุมด้านต่าง ๆ เช่น ความตระหนักด้านความปลอดภัยพื้นฐาน

ลำดับที่	เอกสาร	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
1	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ		การชักชวนแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น นอกจากนี้สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรเสริมสร้างความตระหนักรู้ถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามไซเบอร์ให้กับลูกค้าและผู้ให้บริการอย่างสม่ำเสมอ และต่อเนื่องให้เท่าทันกับความเสี่ยงและภัยคุกคามใหม่ๆ	ความปลอดภัยในการทำงาน การระบุและป้องกันช่องโหว่ การปกป้องความเป็นส่วนตัว การตอบสนองเหตุฉุกเฉิน มาตรฐานความปลอดภัยในการพัฒนา และข้อกำหนดด้านความปลอดภัยของข้อมูล ขั้นตอนการดำเนินการ คู่มือผู้ใช้ และเอกสารอื่น ๆ ของผลิตภัณฑ์ Tencent Cloud ได้รับการจัดทำเป็นลายลักษณ์อักษรและจัดเตรียมไว้สำหรับลูกค้าผ่านทางเว็บไซต์อย่างเป็นทางการ นอกจากนี้ Tencent Cloud ยังมอบบริการ Training and Certification ที่อ้างอิงจากความรู้ทั่วไปเกี่ยวกับผลิตภัณฑ์ Tencent Cloud และความสามารถทางวิชาชีพที่เกี่ยวข้อง เพื่อเสริมสร้างความสามารถทางเทคนิคและความคล่องแคล่วในการใช้ระบบคลาวด์ของลูกค้า

5.3 เอกสารแนบ 2

การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

ลำดับที่	เอกสาร	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
1	2.1.1-2.1.7	การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ	บริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เหมาะสม โดยต้องจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถระบุรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน และสามารถนำไปใช้กำหนดแนวทางการรักษา	ลูกค้าควรบำรุงรักษาบัญชีรายการสินทรัพย์ที่ประกอบด้วยสินทรัพย์ข้อมูลทั้งหมด และสร้างกลไกการจัดการสินทรัพย์ข้อมูลเพื่อระบุสินทรัพย์ จัดระดับและหมวดหมู่ กำหนดกรรมสิทธิ์ในสินทรัพย์ และจัดการความปลอดภัยของสินทรัพย์ตามระดับที่แตกต่างกัน บัญชีรายการสินทรัพย์ควรได้รับการทบทวนเป็นประจำ และควรได้รับการปรับปรุงให้ทันสมัยทันทีเมื่อมีการเปลี่ยนแปลง เพื่อช่วยเหลือลูกค้าในการบริหารสินทรัพย์ข้อมูลอย่าง

เอกสาร รแนบ 2	ลำดับที่ แนวปฏิบัติในการบริ หารความเสี่ยงด้านเท คโนโลยีสารสนเทศ	โดเมน การคว การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
			ษาความมั่นคงปลอดภัย ยด้านเทคโนโลยี สารสนเทศได้อย่างเหม าสม นอกจากนี้ ต้องบำรุงรักษาทรัพย์สิน ด้านเทคโนโลยีสารสนเทศ อย่างสม่ำเสมอ รวมถึงบริหารจัดการท รัพย์สินด้านเทคโนโลยี สารสนเทศที่ใกล้หมด อายุการใช้งานหรือสิ้นสุด การให้บริการ อย่างเหมาะสมและเท่า ทันกับความเสี่ยง เพื่อให้ระบบเทคโนโลยี สารสนเทศมีความมั่น คงปลอดภัย พร้อมใช้งานและสามารถ รองรับการให้บริการ หรือดำเนินธุรกิจได้ย าวต่อเนื่อง	ครอบคลุม Tencent Cloud Cloud Workload Protection Platform (CWPP) ซึ่งสนับสนุนการรวบรวมลายเซ็นดิจิทัลของสินทรัพย์โดยอัตโนมัติ และบริหารจัดการข้อมูลลายเซ็นดิจิทัลของสินทรัพย์ เช่น บัญชีผู้ใช้ พอร์ต กระบวนการ และแอปพลิเคชัน อย่างเป็นเอกภาพ CWPP ยังสามารถดำเนินการตรวจสอบอย่างรวดเร็วเกี่ยวกับขอบเขตผลกระทบความเสี่ยงของเหตุการณ์ความปลอดภัยที่เกิดขึ้นแล้ว ตามลายเซ็นดิจิทัลของสินทรัพย์ เพื่อช่วยลูกค้ายกระดับความปลอดภัยของเซิร์ฟเวอร์ ลูกค้ายังสามารถใช้แพลตฟอร์มการจัดการความปลอดภัยแบบครบวงจร Cloud Security Center (CSC) ของ Tencent Cloud เพื่อบริหารจัดการความปลอดภัยของสินทรัพย์ข้อมูล CSC มีฟังก์ชันศูนย์ความปลอดภัยสินทรัพย์ ซึ่งช่วยให้ลูกค้าสามารถตรวจสอบสินทรัพย์บนคลาวด์แบบไดนามิกโดยอัตโนมัติ รวมถึงเซิร์ฟเวอร์คลาวด์ ที่เก็บวัตถุ ฐานข้อมูลคลาวด์ โหลดบาลานเซอร์ เป็นต้น และบริหารจัดการความเสี่ยงด้านความปลอดภัยของสินทรัพย์แบบครบวงจรผ่านหลายมิติความปลอดภัย เช่น ความเสี่ยงการกำหนดค่าคลาวด์ ช่องโหว่ และเหตุการณ์ความปลอดภัย เพื่อลดความเสี่ยง "IT ล่องหน" บนคลาวด์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดมาตรฐานการจัดการสินทรัพย์ข้อมูลและกระบวนการจัดการตลอดวงจรชีวิตสินทรัพย์ เพื่อจัดการและปกป้องสินทรัพย์ เช่น ข้อมูลอิเล็กทรอนิกส์ ฮาร์ดแวร์และอุปกรณ์เสมือน โครงสร้างพื้นฐาน ระบบแอปพลิเคชัน และซอฟต์แวร์ โดยจำแนกประเภทและระดับ Tencent Cloud ใช้ระบบการจัดการสินทรัพย์ในการบริหารจัดการอุปกรณ์ฮาร์ดแวร์และส่วนประกอบซอฟต์แวร์ รวมถึงการลงทะเบียนและผูกมัดสินทรัพย์ การตรวจสอบและการอัปเดตข้อมูลสินทรัพย์ การปลดระวางและเปลี่ยนใหม่สินทรัพย์ เป็นต้น เพื่อรับประกันการทำงานที่ราบรื่นของระบบพื้นฐานของ

ลำดับที่		โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
2	2.2.1-2.2.9	การรักษาความมั่นคงปลอดภัยของข้อมูลทั้งการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารและ การจัดเก็บข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ มีการจัดชั้นความลับของข้อมูล (information classification) เก็บรักษาและทำลายข้อมูลให้เหมาะสมตามระดับชั้นความลับ รวมทั้งบริหารจัดการการเข้ารหัสข้อมูล (cryptography) ที่เชื่อถือได้และเป็นมาตรฐานสากลที่ยอมรับโดยทั่วไป เพื่อรักษาความมั่นคงปลอดภัยและความลับของข้อมูล	แพลตฟอร์มคลาวด์และจัดเตรียมการสนับสนุนที่เชื่อถือได้ให้กับระบบธุรกิจ สำหรับฮาร์ดแวร์ที่ปลดระวางแล้ว Tencent Cloud ใช้วิธีการทำลายทางกายภาพที่ปลอดภัย เพื่อรับประกันว่าฮาร์ดแวร์ถูกทำลายอย่างสมบูรณ์ และมีการบันทึกการไว้ในบันทึกการทำลาย ลูกค้าควรกำหนดกลไกการปกป้องความปลอดภัยของข้อมูล โดยจำแนกประเภทข้อมูลตามระดับความอ่อนไหวและความสำคัญ และดำเนินการมาตรการป้องกันข้อมูลตามระดับข้อมูลที่แตกต่างกัน ใช้มาตรฐานการเข้ารหัสที่เชื่อถือได้และยอมรับในระดับสากล เพื่อปกป้องความเป็นความลับและความสมบูรณ์ของข้อมูล เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการจำแนกประเภทและระดับข้อมูล Data Security Governance Center (DSGC) สามารถช่วยลูกค้าจัดการสินทรัพย์ข้อมูลโดยอัตโนมัติจัดประเภทและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลขององค์กรบนคลาวด์ โดยได้รับอนุญาตจากองค์กร DSGC จะเชื่อมต่อกับสินทรัพย์ข้อมูลประเภทต่างๆบนคลาวด์อย่างลึกซึ้ง และรับข้อมูลสินทรัพย์ข้อมูลที่ทันเวลาจากมิติภายในตามลักษณะของข้อมูล DSGC จะช่วยองค์กรค้นพบข้อมูลที่ละเอียดอ่อนอย่างเจาะจงและจัดระเบียบสินทรัพย์ข้อมูลจากมุมมองความปลอดภัย ตามมาตรฐานการจำแนกประเภทและระดับข้อมูลระดับชาติ อุตสาหกรรม หรือองค์กร DSGC จะช่วยองค์กรในการจำแนกประเภทและระดับข้อมูล เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานการจำแนกประเภทและระดับข้อมูลที่สมบูรณ์ภายในองค์กร	

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโณโลยีสารสนเทศ			โดยข้อมูลทั้งหมดจะถูกจำแนกประเภทและระดับตามมา ตรฐานนี้อย่างเป็นเอกภาพตั้งแต่เริ่มสร้าง ข้อมูลของลูกค้าภายใน Tencent Cloud จัดอยู่ในระดับความปลอดภัยสูง สำหรับพนักงานภายใน Tencent Cloud หากไม่ใช้บริการที่ลูกค้าเลือกใช้ซึ่งจำเป็นต้องประมวลผล ข้อมูลของลูกค้า พนักงาน Tencent Cloud จะไม่พยายามเข้าถึงข้อมูลลูกค้าใดๆ Tencent Cloud ได้สร้างมาตรฐานการจำแนกประเภทและระดับข้อมูลที่ สมบูรณ์ภายในองค์กร โดยข้อมูลทั้งหมดจะถูกจำแนกประเภทและระดับตามมา ตรฐานนี้อย่างเป็นเอกภาพตั้งแต่เริ่มสร้าง ข้อมูลของลูกค้าภายใน Tencent Cloud จัดอยู่ในระดับความปลอดภัยสูง สำหรับพนักงานภายใน Tencent Cloud หากไม่ใช้บริการที่ลูกค้าเลือกใช้ซึ่งจำเป็นต้องประมวลผล ข้อมูลของลูกค้า พนักงาน Tencent Cloud จะไม่พยายามเข้าถึงข้อมูลลูกค้าใดๆ ในด้านการป้องกันการจัดเก็บข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการ ของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสานรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความปลอดภัยของข้อมูล Key Management Service (KMS) ใช้โมดูลความปลอดภัยฮาร์ดแวร์ (HSM) ที่ได้รับการรับรอง FIPS-140-2 ในการสร้างและปกป้องคีย์ และสามารถสนับสนุนการจัดการวงจรชีวิตเต็มรูปแบบ ของคีย์การเข้ารหัสของลูกค้า เพื่อลดความเสี่ยงที่คีย์อาจถูกเจาะหรือนำไปใช้ในทาง ที่ผิด KMS รองรับการหมุนเวียนคีย์ และใช้วิธีการลบคีย์ที่หมดอายุ ถูกยกเลิก หรือรั่วไหลออกไปอย่างปลอดภัยและเชื่อถือได้ คีย์ที่ถูกลบไปแล้วไม่สามารถกู้คืนได้

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโนโลยีสารสนเทศ			และข้อมูลที่เข้ารหัสภายใต้คีย์นั้นจะไม่สามารถถอดรหัสได้เช่นกัน นอกจากนี้ Tencent Cloud ใช้เทคโนโลยีการจับกุมข้อมูลสำรองหลายชุดและการเข้ารหัสลับล้างข้อผิดพลาดเมื่อจับกุมข้อมูลและดำเนินการกู้คืนที่จำเป็นเมื่อตรวจพบข้อผิดพลาดด้านความสมบูรณ์ ซึ่งช่วยเพิ่มขีดความสามารถในการทนต่อข้อผิดพลาดของข้อมูลอย่างมาก ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจถึงความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า นอกจากนี้ ลูกค้ายังสามารถใช้บริการ Tencent Cloud ต่อไปเพื่อให้บรรลุการถ่ายโอนข้อมูลที่ปลอดภัยในสถานการณ์ต่างๆ: Direct Connect (DC): จัดเตรียมการเชื่อมต่อเครือข่ายแบนด์วิดท์สูงที่มีความเฉพาะตัวและความปลอดภัยสูง ผู้ใช้เป็นเจ้าของลิงก์เครือข่ายโดยเฉพาะ ไม่มีความเสี่ยงข้อมูลรั่วไหล VPN Connection: อิงตามเทคโนโลยีอุโมงค์เครือข่าย เพื่อให้บรรลุการถ่ายโอนข้อมูลที่ปลอดภัยระหว่างศูนย์ข้อมูลในพื้นที่และทรัพยากรบน Tencent Cloud อุโมงค์ VPN ใช้ IKE (โปรโตคอลแลกเปลี่ยนคีย์ลับ) และ IPsec เพื่อเข้ารหัสข้อมูลที่ถ่ายโอน สร้างอุโมงค์ข้อมูลที่ปลอดภัยและนำเชื่อถือบนอินเทอร์เน็ต เพื่อปกป้องความปลอดภัยของข้อมูลระหว่างการถ่ายโอน

สำหรับการลบและทำลายข้อมูล Tencent Cloud

ลำดับที่		โดเมน การควบคุม	ข้อกำหนดความ เฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ รณ			
2	ความปลอดภัยสารสนเทศ			มีกลไกทำลายข้อมูลที่ปลอดภัยและเชื่อถือได้ เมื่อบริการของลูกค้าหมดอายุลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรอง อย่างสิ้นเชิงหลังจากเวลาเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้ เมื่อผู้ใช้ให้บริการ Tencent Cloud เกิดความขัดข้องและจำเป็นต้องเปลี่ยนหรือถึงอายุการ ใช้งานและจำเป็นต้องกำจัด Tencent Cloud จะลบข้อมูลที่เหลืออยู่ทันที และปฏิบัติตามขั้นตอนที่เข้มงวดเพื่อทำลายทางกายภาพ อย่างสมบูรณ์ในเวลาที่เหมาะสม ในด้านการจัดการคีย์ Tencent Cloud ยังได้กำหนดมาตรฐานการเข้ารหัสและการจัดการคีย์ โดยกำหนดข้อกำหนดด้านความปลอดภัยสำหรับกระบวน การต่างๆ ในการสมัครคีย์ การสร้าง การจัดเก็บ การใช้ การส่งต่อ การอัปเดต และการทำลายคีย์ การดำเนินการต่างๆ ที่เกี่ยวข้องกับวงจรชีวิตของคีย์ทั้งหมดต้องปฏิบัติตาม ข้อกำหนดพื้นฐานของการควบคุมสองชั้น การส่งมอบที่เข้มงวด การเก็บรักษาที่เหมาะสม และการอัปเดตที่ทันทั่วทั้ง กระบวนการใช้คีย์ยังต้องแน่ใจว่าปฏิบัติตามข้อกำหนด เช่น การแยกหน้าที่และความรับผิดชอบ การอนุมัติที่เข้มงวด และการดำเนินการด้วยชื่อจริง และต้องเก็บรักษาบันทึกการดำเนินการคีย์ทางธุรกิจ และดำเนินการตรวจสอบการดำเนินการเป็นประจำ นอกจากนี้ ในกระบวนการใช้อัลกอริธึมการเข้ารหัสระหว่างการถ่าย โอนและการจัดเก็บข้อมูล Tencent Cloud กำหนดให้ทีมงานภายในปฏิบัติตามมาตรฐานหรือกฎระ เบียบที่เกี่ยวข้องกับการจัดการรหัสผ่านสากล เลือกใช้อัลกอริธึมระดับความปลอดภัยสูง เช่น AES- 256 และให้แน่ใจว่าความยาวของคีย์เป็นไปตามข้อกำหนด
3.1, 3.2	2.3.1-2.3.4	การควบคุมการเข้าถึง	ต้องควบคุมการเข้าถึง ระบบปฏิบัติการ ระบบงาน และระบบฐานข้อมูล	ลูกค้าควรสร้างกลไกการพิสูจน์ตัวตนและความคุ้มครองเข้าถึงสำหรับข้อมูลและระบบเทคโนโลยีสารสนเทศเพื่อควบคุมการเข้าถึงสินทรัพย์ข้อมูล ทบทวนและอัปเดตสิทธิ์เป็นประจำ

เอกสาร รแบบ 2	ลำดับที่ แนวปฏิบัติในการบริ หารความเสี่ยงด้านเท คโนโลยีสารสนเทศ	โดเมน การคว มคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
			โดยกำหนดให้ มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มสิทธิ โดยต้องครอบคลุมอย่างน้อย ดังนี้ บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user) ต้องมีการกำหนดมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานที่มีสิทธิสูงอย่างเข้มงวด เช่น การมอบหมายสิทธิการเปิดใช้ กำหนดระยะเวลาการใช้งาน การสอบทานหลังการไ ซ์ เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มสิทธิ หรือไม่ได้รับอนุญาต จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้ (1) บัญชีผู้ใช้งานที่มีสิทธิสูง (privileged user)	และเสริมสร้างการจัดการความปลอดภัยของบัญชีผู้ใช้ที่มีสิทธิพิเศษโดยใช้การพิสูจน์ตัวตนหลายปัจจัยและกลไกการตรวจสอบ ในด้านการจัดการบัญชีผู้ใช้และการอนุญาต Cloud Access Management (CAM) สามารถช่วยลูกค้าจัดการการเข้าถึงผลิตภัณฑ์และบริการ Tencent Cloud อย่างปลอดภัยและละเอียดรอบคอบ ผู้ใช้สามารถแก้ไขกฎรหัสผ่านของผู้ใช้ย่อยผ่านคอนโซลการจัดการการเข้าถึง รวมถึงความซับซ้อนของรหัสผ่าน ความยาว ระยะเวลาที่มีผล เป็นต้น เพื่อป้องกันไม่ไห้รหัสผ่านรั่วไหล Tencent Cloud จะใช้การเข้ารหัสแฮช SHA256 และการเติมเกลือ (Salt) สำหรับรหัสผ่านของลูกค้า เพื่อหลีกเลี่ยงการเก็บรหัสผ่านในรูปแบบข้อความธรรมดา CAM ยังสนับสนุนฟังก์ชันการตรวจสอบยืนยันตัวตนขั้นที่สองหลายวิธี รวมถึงการใช้การตรวจสอบโดยอุปกรณ์ MFA หรือการตรวจสอบด้วยรหัสยืนยันทางโทรศัพท์ เพื่อยืนยันความปลอดภัยของตัวตนและสภาพแวดล้อมก่อนเข้าสู่ระบบและดำเนินการที่ละเอียดอ่อน Tencent Cloud ยังได้กำหนดกลยุทธ์การอนุมัติสำหรับการควบคุมการเข้าถึงและกลไกเมทริกซ์การแยกอำนาจภายในองค์กร โดยกำหนดให้บัญชีผู้ใช้ต้องใช้ตัวระบุเฉพาะ และตั้งค่านโยบายรหัสผ่านสำหรับบัญชีพนักงานตามแนวทางความปลอดภัยขั้นพื้นฐาน ซึ่งรวมถึงความยาวรหัสผ่าน ความซับซ้อน การลือคและการรีเซต เป็นต้น สำหรับอุปกรณ์ปลายทาง ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายภายใน Tencent Cloud ได้กำหนดค่าการจำกัดจำนวนครั้งในการเข้าสู่ระบบที่ล้มเหลวและนโยบายหมดเวลาการทำงานของเซสชัน Tencent Cloud ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการตรวจสอบสิทธิการเข้าถึงของพนักงาน โดยผู้ใช้ต้องผ่านการยืนยันตัวตนสองปัจจัยก่อนเข้าถึงทรัพยากรภายใน Tencent Cloud

ลำดับที่		โดเมน การคว มคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโนโลยีสารสนเทศ		ทุกบัญชีของระบบปฏิบัติการ ระบบ ฐานข้อมูล ระบบงาน อุปกรณ์เครือข่ายและ อุปกรณ์รักษาความปลอดภัย ออดภัยเครือข่าย (2) บัญชีผู้ใช้งาน (user) ทุกบัญชีที่สามารถเข้าถึงข้อมูลลูกค้าและเชื่อมต่อไปมาจากระบบ เครือข่ายสื่อสารสาธารณะ	ปฏิบัติตามหลักการสิทธิ์น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิ์น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิ์เฉพาะที่ต่อเมื่อมีความจำเป็นต้องใช้ และผ่านกระบวนการอนุมัติสิทธิ์ที่เข้มงวดเท่านั้น Tencent Cloud จะรักษามั่นทอนข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดการตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์ สำหรับผู้ที่มีสิทธิ์สูง ลูกค้าสามารถใช้ Cloud Access Management (CAM) เพื่อมอบสิทธิ์การเข้าถึงทรัพยากรให้กับผู้ใช้ย่อยผ่านวิธีการต่างๆ เช่น แท็ก เพื่อให้บรรลุการควบคุมการเข้าถึงทรัพยากรคลาวด์อย่างละเอียด CAM ยังสนับสนุนการดูและติดตามบันทึกการดำเนินการของพนักงานผ่าน CloudAudit นอกจากนี้ Tencent Cloud ยังให้บริการ Bastion Host (BH) ที่สามารถสนับสนุนการอนุญาตอย่างละเอียดตามมิติต่างๆ เช่น ผู้ใช้ สินทรัพย์ บัญชีผู้ใช้ และสิทธิ์การดำเนินการ เพื่อให้มั่นใจว่าสิทธิ์ที่ผู้ใช้มีอยู่เป็นสิทธิ์ขั้นต่ำที่จำเป็นสำหรับการเข้าถึงสินทรัพย์และทำงานให้สำเร็จ เครื่องบินคุ้มกัน ยังสนับสนุนฟังก์ชันการตรวจสอบการดำเนินการโดยบันทึกและวิเคราะห์บันทึกการดำเนินการของผู้ใช้ เพื่อให้มั่นใจว่าสามารถติดตามเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพ ภายใน Tencent Cloud ยังได้กำหนดข้อกำหนดการจัดการสำหรับสิทธิ์การเข้าถึงพิเศษและสร้างกลไกการอนุญาตที่เกี่ยวข้องในเวลาเดียวกัน Tencent Cloud ได้ปรับใช้เครื่องบินคุ้มกัน อย่างเต็มที่ในสภาพแวดล้อมการผลิต โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบแบ็กเอนด์จากส่วนกลางผ่าน เครื่องบินคุ้มกัน การเข้าถึง เครื่องบินคุ้มกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติการอนุญาต เจ้าหน้าที่ปฏิบัติการภายในบางส่วนของ

ลำดับที่		โดเมน การควบคุม	ข้อกำหนดควบคุม เฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโณโลยีสารสนเทศ			Tencent Cloud เท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบ เครื่องบินคัมกัน ต้องการการยืนยันตัวตนสองปัจจัย ในด้านการเฝ้าระวังความปลอดภัยของบัญชี <u>Cloud Access Management (CAM)</u> ผ่านฟังก์ชันการควบคุมสิทธิ์อย่างละเอียดอ่อน มอบสิทธิ์เฉพาะให้กับบุคลากรต่างๆ สำหรับทรัพยากรที่แตกต่างกัน ลูกค้ายังสามารถดูและติดตามบันทึกการดำเนินการของพนักงานผ่าน <u>CloudAudit</u> รองรับการดูบันทึกการดำเนินการของคอนโซล Tencent Cloud และ API คลาวด์ภายใน 90 วันออนไลน์ ข้อมูลลูกค้าภายใน Tencent Cloud จัดอยู่ในระดับความปลอดภัยสูง สิทธิ์ควบคุมข้อมูลลูกค้าอยู่ในความครอบครองของลูกค้าโดยสมบูรณ์ Tencent Cloud จะไม่พยายามเข้าถึงหรือเปิดเผยเนื้อหาของลูกค้า หากลูกค้ามีข้อสงสัยใดๆ เกี่ยวกับบัญชี ความปลอดภัยเครือข่าย หรือปัญหาการใช้ผลิตภัณฑ์ สามารถส่งใบงานผ่านคอนโซลเพื่อรับการสนับสนุนทางเทคนิค Tencent Cloud มีกลไกการรับประกันความปลอดภัยในการปฏิบัติการที่ครบถ้วน เพื่อให้มั่นใจว่าทีมบริการปฏิบัติการไม่สามารถเข้าถึงสินทรัพย์ข้อมูลของลูกค้าได้โดยตรง หากไม่ได้รับความยินยอมและการอนุญาตจากลูกค้า สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้ เครื่องบินคัมกัน อย่างเต็มที่ การดำเนินการที่ละเอียดอ่อนในสภาพแวดล้อมการผลิตทั้งหมดต้องเข้าถึงผ่านการเข้าสู่ระบบ เครื่องบินคัมกัน แบบเรียลไทม์ และบันทึกการเข้าสู่ระบบและบันทึกการดำเนินการทั้งหมดจะถูกรวบรวมไปยังแพลตฟอร์มการจัดการบันทึก (log) ของ Tencent Cloud เพื่อเก็บรักษาในรูปแบบเข้ารหัส ผ่านเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติการและทีมตรวจสอบภายในจะทำการตรวจสอบบันทึก (log)

ลำดับที่		โดเมน การคว มคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ หารแนว			
2	ความปลอดภัยด้านเท คโนโลยีสารสนเทศ			เพื่อตรวจสอบความผิดปกติของระบบหรือการดำเนินการ เพื่อป้องกันความเสี่ยงในการปฏิบัติการ
4	2.4.1-2.4.3	การรักษา ความมั่น คงปลอด ภัยทางก ายภาพแ ละสภาพ แวดล้อม	รักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับ เทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับ เทคโนโลยีสารสนเทศ ที่สำคัญ รวมทั้งมีระบบป้องกัน การรั่ว ความมั่น คงปลอด ภัยทางก ายภาพแ ละสภาพ แวดล้อม และกระบวนการบำรุงร กษาอุปกรณ์คอมพิวเตอร์ และระบบสารสนเทศ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากกา รบุกรุกหรือจากภัยธรรมชาติ และให้มีความพร้อมใช้ งานสามารถ รองรับการให้บริการหรือ ดำเนินการธุรกิจอย่างต่อเนื่อง	ลูกค้าควรสร้างกลไกการควบคุมความปลอดภัยทางกายภาพและสิ่งแวดล้อมสำหรับสินทรัพย์เทคโนโลยีสารสนเทศ และดำเนินการป้องกันการความปลอดภัยและการบำรุงรักษาเป็นประจำสำหรับอุปกรณ์ฮาร์ดแวร์และโครงสร้างพื้นฐานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจในความปลอดภัยของสินทรัพย์ โครงสร้างพื้นฐานของ Tencent Cloud มีการกระจายตัวอยู่ในหลายสถานที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) ภูมิภาค (region) แต่ละแห่งเป็นพื้นที่ทางภูมิศาสตร์อิสระ ในขณะที่โซนความพร้อมใช้งานแต่ละโซนเป็นโดเมนการบำรุงรักษาความล้มเหลวอิสระ และแต่ละโซนความพร้อมใช้งานถูกแยกจากกันทางกายภาพ ลูกค้าสามารถปรับใช้ข้อมูลและระบบในภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างยืดหยุ่นตามความต้องการในการพัฒนาธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติทางธุรกิจ ในด้านความปลอดภัยของสภาพแวดล้อมศูนย์ข้อมูล ศูนย์ข้อมูลทั้งหมดของ Tencent Cloud ทั่วโลกดำเนินการเลือกที่ตั้ง ก่อสร้าง หรือเช่าตามมาตรฐานสากลที่เกี่ยวข้องและข้อกำหนดความปลอดภัยในท้องถิ่น ทั้งระบบไฟฟ้าและระบบปรับอากาศของแต่ละศูนย์ข้อมูล ออกแบบด้วยความเสถียรสูงและแบบซ้ำซ้อนเต็มรูปแบบ ความล้มเหลวของจุดใดจุดหนึ่งจะไม่ส่งผลกระทบต่อความต่อเนื่องของไฟฟ้าและการระบายความร้อนของศูนย์ข้อมูล แต่ละศูนย์ข้อมูลติดตั้งระบบดับเพลิงครบถ้วน รวมถึงระบบตรวจจับไฟในพื้นที่จุดเฉพาะ ระบบดับเพลิงอัตโนมัติ และอุปกรณ์ดับเพลิงด้วยมือสำหรับใช้ในกรณีฉุกเฉิน

ลำดับที่		โดเมน การคว มคุม	ข้อกำหนดควม เฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโนโลยีสารสนเทศ			ภายในศูนย์ข้อมูลแต่ละแห่งติดตั้งพื้นป้องกันไฟฟ้าสถิต ผู้รับ และรางสายไฟทั้งหมดติดตั้งสายกราวด์เพื่อป้องกันความ เสียหายต่ออุปกรณ์จากไฟฟ้าสถิต ในด้านการควบคุมการเข้าถึงศูนย์ข้อมูล Tencent Cloud ได้กำหนดขั้นตอนการเข้าถึงที่เป็นทางการสำหรับการ เข้าถึงทางกายภาพของศูนย์ข้อมูล บุคคลที่ต้องการเข้าสู่ศูนย์ข้อมูลต้องแสดงตัวตนและนำ หลักฐานแสดงตัวตนมายื่นต่อเจ้าหน้าที่ปฏิบัติการคว มปลอดภัย ผู้จัดการศูนย์ข้อมูลแต่ละแห่งต้องบันทึกและจัดการการ มอบสิทธิ์ การแก้ไข และการยกเลิกสิทธิ์การเข้าถึงในระบบการเข้าถึงศูนย์ข อมูลภายในของตน ผู้จัดการศูนย์ข้อมูลจะทบทวนสิทธิ์การเข้าถึงศูนย์ข อมูลเป็นประจำ เพื่อให้มั่นใจว่าการจัดสรรสิทธิ์การเข้าถึงอย่างเหมาะสม หากสิทธิ์การเข้าถึงไม่เกี่ยวข้องหรือไม่จำเป็นอีกต่อไป ผู้จัดการศูนย์ข้อมูลของ Tencent Cloud จะปิดการใช้งานสิทธิ์การเข้าถึงดังกล่าว ผู้เยี่ยมชมที่ได้รับอนุมัติให้เข้าสู่ศูนย์ข้อมูลของ Tencent Cloud ล้วนได้รับการดูแลโดยวิศวกรภาคสนามของ Tencent Cloud ผู้เยี่ยมชมหรือพนักงานทุกประเภทที่เข้าออกศูนย์ข อมูลต้องได้รับการตรวจสอบตัวตนและตรวจสอบสัมภาระที่ พกพา และลงทะเบียนสิ่งของที่นำติดตัวมา ในด้านการตรวจสอบและเฝ้าระวังศูนย์ข้อมูลแล ะการตรวจสอบประจำวัน การจัดการการเฝ้าระวังศูนย์ข้อมูลของ Tencent Cloud ครอบคลุมพื้นที่ภายในห้องเซิร์ฟเวอร์แต่ละแห่ง พื้นที่ส่งมอบงาน จุดเข้าออกพื้นที่ศูนย์ข้อมูล และจุดเข้าออกอาคารต่างๆ ภายในพื้นที่ศูนย์ข้อมูล ซึ่งทั้งหมดติดตั้งระบบแจ้งเตือนการเฝ้าระวังด้วยวิดีโอแ บบไม่มีจุดบอด 24 ชั่วโมงตลอด 7 วัน และมีเจ้าหน้าที่รักษาความปลอดภัยประจำการ 24 ชั่วโมงตลอด 7 วัน

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ รแบบ			
2	ความปลอดภัยด้านเท คโนโลยีสารสนเทศ			เจ้าหน้าที่รักษาความปลอดภัยของศูนย์ข้อมูลแต่ละแห่งของ Tencent Cloud ดำเนินการตรวจสอบสถานการณ์ของห้องเซิร์ฟเวอร์และอุปกรณ์ต่างๆ อย่างเคร่งครัดตามรายการตรวจสอบและแผนการตรวจสอบ โดยครอบคลุมพื้นที่ต่างๆ เช่น จุดเข้าออกอาคาร บริเวณรอบอาคาร และภายในอาคาร พร้อมทั้งลงนาม ณ จุดตรวจและบันทึกเวลาในการตรวจสอบ ทันทีที่พบความขัดข้องของโครงสร้างพื้นฐานหรือเหตุการณ์ด้านความปลอดภัย จะเริ่มต้นขั้นตอนการตอบสนองเหตุฉุกเฉินของศูนย์ข้อมูลทันที ในด้านการฝึกซ้อมความปลอดภัยทางกายภาพของศูนย์ข้อมูล ศูนย์ข้อมูลแต่ละแห่งได้กำหนดแผนการตอบสนองฉุกเฉินด้านความปลอดภัยทางกายภาพ และจัดให้เจ้าหน้าที่ศูนย์ข้อมูลฝึกซ้อมด้านความปลอดภัยเป็นประจำ ทันทีที่เกิดเหตุการณ์ด้านความปลอดภัยทางกายภาพ แผนดังกล่าวจะมีผลบังคับใช้ทันทีและชี้ให้ผู้เกี่ยวข้องให้ปกป้องสินทรัพย์ของลูกค้าให้ได้มากที่สุดเท่าที่จะเป็นไปได้ เหตุการณ์ด้านความปลอดภัยทั้งหมดจะถูกบันทึกและวิเคราะห์โดยละเอียด เพื่อใช้ในการปรับปรุงและยกระดับมาตรฐานและระบบการจัดการความปลอดภัยที่มีอยู่อย่างต่อเนื่อง นอกจากนี้ Tencent Cloud ยังดำเนินการตรวจสอบและตรวจสอบศูนย์ข้อมูลภาคสนามเป็นประจำ เพื่อให้แน่ใจว่าศูนย์ข้อมูลเป็นไปตามข้อกำหนดด้านความปลอดภัยข้อมูลที่ Tencent Cloud กำหนด Tencent Cloud ทบทวนผลการประเมินความเสี่ยงด้านภัยคุกคามและช่องโหว่ (TVRA) ที่ดำเนินการโดยผู้ให้บริการศูนย์ข้อมูล เพื่อให้มั่นใจในประสิทธิภาพของมาตรการจัดการที่เกี่ยวข้อง
5	2.5.1.-2.5.17	การรักษา ความม ั่นคงปลอดภัย	รักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร	ลูกค้าควรกำหนดและดำเนินการขั้นตอนเกี่ยวกับเครือข่าย การสื่อสารเพื่อป้องกันการเชื่อมต่อเครือข่ายที่ไม่ปลอดภัย

เอกสารแนบ	ลำดับที่	โดเมนการควบคุม	ข้อกำหนดความคุ้มครองเฉพาะ	การตอบสนองของ Tencent Cloud
2	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ภัยของระบบเครือข่ายสื่อสารข้อมูลที่ได้รับส่งผ่านระบบเครือข่ายสื่อสารมีควมมั่นคงปลอดภัยสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น รวมทั้งพร้อมรองรับการให้บริการได้อย่างต่อเนื่อง	เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่ได้รับส่งผ่านระบบเครือข่ายสื่อสารมีควมมั่นคงปลอดภัยสามารถป้องกันการบุกรุกหรือภัยคุกคามที่อาจเกิดขึ้น รวมทั้งพร้อมรองรับการให้บริการได้อย่างต่อเนื่อง	ดำเนินการหรือติดตั้งมาตรการหรืออุปกรณ์ความปลอดภัยเครือข่ายที่จำเป็น เพื่อปกป้องระบบเครือข่ายและเฝ้าระวังภัยคุกคามและบุกรุกความปลอดภัยเครือข่ายได้อย่างทันที่ เครือข่ายพื้นฐานของ Tencent Cloud ใช้วิธีการก่อสร้างแบบซ้ำซ้อน ร่วมกับการจัดลำดับความสำคัญของเส้นทางในระดับการกำหนดเส้นทางและการจัดสรรการจราจรเพื่อความสามารถในการเข้าถึงเส้นทาง เพื่อให้มั่นใจว่าบริการเครือข่ายจะไม่หยุดชะงักเนื่องจากความล้มเหลวของอุปกรณ์ใดๆ โหนดการคำนวณของ Tencent Cloud ยังใช้วิธีการก่อสร้างแบบซ้ำซ้อน โดยเมื่อโหนดการคำนวณเดียวเกิดความล้มเหลวจะถูกตัดออกโดยอัตโนมัติแบบเรียลไทม์ผ่านตัวจัดกำหนดการ ซึ่งรับประกันความพร้อมใช้งานของธุรกิจลูกค้าได้อย่างมีประสิทธิภาพ ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจก็มีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า <u>Direct Connect (DC)</u>: จัดเตรียมการเชื่อมต่อเครือข่ายแบนด์วิดท์สูงที่มีความเฉพาะตัวและความปลอดภัยสูง ผู้ใช้เป็นเจ้าของลิงก์เครือข่ายโดยเฉพาะ ไม่มีความเสี่ยงข้อมูลรั่วไหล นอกจากนี้ ลูกค้ายังสามารถใช้ <u>Cloud Connect Network (CCN)</u> เพื่อให้บริการการเชื่อมต่ออินเทอร์เน็ตที่ปลอดภัยระหว่าง Virtual Private Cloud (VPC) บนคลาวด์ และระหว่าง VPC กับศูนย์ข้อมูลในพื้นที่ (IDC) สำหรับข้อกำหนดการแบ่งส่วนเครือข่าย ลูกค้าสามารถใช้บริการ <u>Virtual Private Cloud</u>

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบปฏิบัติการในการบริหารแนวความเสี่ยงด้านเทคโนโลยีสารสนเทศ 2			(VPC) ที่ Tencent Cloud ให้มาเพื่อสร้างพื้นที่เครือข่ายอิสระหลายแห่งสำหรับทรัพยากรแพลตฟอร์มคลาวด์ที่ได้ซื้อไปแล้ว และกำหนดการแบ่งส่วนเครือข่ายและที่อยู่ IP นโยบายการกำหนดเส้นทาง ฯลฯ ตามต้องการได้ด้วยตนเอง บริการ VPC เป็นพื้นที่เครือข่ายบนคลาวด์เฉพาะที่สร้างขึ้นบน Tencent Cloud โดยเครือข่ายส่วนตัวใช้เทคโนโลยีโมงส์ สร้างเครือข่ายเสมือนบนเครือข่ายกายภาพ และใช้เทคโนโลยีเสมือนจริง เพื่อให้บรรลุการแยกอินทราเน็ตโดยสมบูรณ์ระหว่างเครือข่ายส่วนตัวต่างๆ มอบเครือข่ายคลาวด์ที่ปลอดภัยเป็นอิสระและแยกจากกันให้กับลูกค้า สำหรับเซิร์ฟเวอร์คลาวด์ภายในเครือข่ายส่วนตัว สามารถควบคุมการไหลเข้าออกของข้อมูลในระดับอินสแตนซ์และซับเน็ตได้ผ่านการกำหนดค่ากลุ่มความปลอดภัยและกฎ Access Control List (ACL) ของเครือข่าย เพื่อให้บรรลุการควบคุมการเข้าถึงเครือข่ายในระดับต่างๆ เพื่อดำเนินการป้องกันขอบเขตเครือข่าย Tencent Cloud ให้บริการ EdgeOne (EO) แก่ลูกค้า โดยอิงตามโหนดขอบทั่วโลกของ Tencent Cloud เพื่อบริการป้องกันความปลอดภัยและเร่งความเร็วให้กับลูกค้า มีฟังก์ชัน เช่น การป้องกัน DDoS การป้องกันเว็บอัจฉริยะ การป้องกันการโจมตีประเภทบอท/ครอว์เลอร์ การแก้ไข DNS และสนับสนุนให้ลูกค้าสามารถกำหนดกฎการควบคุมการเข้าถึงแบบกำหนดเองตามความต้องการทางธุรกิจ Cloud Firewall (CFW) ให้การป้องกันขอบเขตเครือข่ายที่แตกต่างกันแก่ลูกค้าเป็นหลัก สนับสนุนการควบคุม ACL ของไฟร์วอลล์อย่างเข้มข้น การปิดกั้น IPS แบบเรียลไทม์ การปะชูดเสมือน และการตรวจจับภัยคุกคามที่เป็นอันตราย ฯลฯ

ลำดับที่		โดเมน การควบคุม	ข้อกำหนดควบคุม เฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริหาร			
รแบบ	หาความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
2	ค			สามารถตอบสนองความต้องการของโซน DMZ ในเครือข่ายแบบดั้งเดิม ปกป้องสินทรัพย์หลักเป็นพิเศษ และบรรลุการควบคุมการแยกอย่างละเอียดระหว่าง VPC Web Application Firewall (WAF) สามารถจัดการกับปัญหาความปลอดภัยของเว็บไซต์และธุรกิจเว็บ เช่น การโจมตีเว็บ การบุกรุก การใช้ประโยชน์จากช่องโหว่ การฝังมัลแวร์ การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต แบ็กดอร์ ครอบครอง ฯลฯ Anti-DDoS ใช้ทรัพยากรป้องกัน DDoS ที่มีคุณภาพและเพียงพอ ร่วมกับอัลกอริทึมการทำความสะอาดที่พัฒนาอย่างต่อเนื่อง "การพัฒนาด้วยตนเอง + การระบุอัจฉริยะด้วย AI" เพื่อจัดการกับปัญหาการโจมตี DDoS สำหรับการแยกหลายผู้เช่า (Multi-tenancy Isolation) Tencent Cloud มีกลไกความปลอดภัย เช่น นโยบายการควบคุมการเข้าถึงทรัพยากรในชั้นควบคุมเสมือน (Virtualization Control Layer) นโยบายการแยกระหว่างเครือข่ายส่วนตัวภายในแพลตฟอร์มคลาวด์ การจัดสรรสิทธิ์และการยืนยันตัวตนบนเว็บคอนโซล รหัสเซสชันของอินเทอร์เน็ตเฟส และศักยภาพเข้าถึง เพื่อให้มั่นใจว่าผู้ใช้แต่ละคนสามารถเข้าถึงทรัพยากรคอมพิวเตอร์คลาวด์ที่ตนซื้อได้เท่านั้น ซึ่งทำให้เกิดการแยกการเข้าถึงระหว่างผู้เช่าหลายรายได้อย่างมีประสิทธิภาพ ในด้านความปลอดภัยของอุปกรณ์เครือข่าย เพื่อให้สอดคล้องกับข้อกำหนดการกำกับดูแลของลูกค้า Tencent Cloud ได้กำหนดมาตรฐานการกำหนดค่าความปลอดภัยเครือข่ายและมาตรฐานเส้นฐานความปลอดภัยขึ้น เพื่อจัดการมาตรฐานการกำหนดค่าความปลอดภัยของอุปกรณ์เครือข่าย ไฟร์วอลล์ ระบบปฏิบัติการของเซิร์ฟเวอร์โฮสต์ ฐานข้อมูล และระบบแอปพลิเคชัน Tencent Cloud ใช้เครื่องมือสแกนเพื่อตรวจจับความเบี่ยงเบนของการกำหนดค่าระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และอิมเมจเสมือน (Virtual Image)

ลำดับที่		โดเมน การคว มคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ หารแนว			
2	ความปลอดภัยด้านเท คโนโลยีสารสนเทศ			จากมาตรฐานอย่างต่อเนื่อง สำหรับความเป็ยเบนที่ตรวจพบ Tencent Cloud จะสร้างใบงานความปลอดภัยและส่งไปยังทีมงานผู้รับผิดชอบโดยอัตโนมัติ เพื่อดำเนินการแก้ไขทันทีที่ Tencent Cloud ยังทบทวนนโยบายความปลอดภัยและการตั้งค่าพารามิเตอร์ของอุปกรณ์เครือข่าย เช่น เราเตอร์ไฟร์วอลล์และเซิร์ฟเวอร์เครือข่าย เป็นระยะ เพื่อให้มั่นใจในประสิทธิผลของนโยบายและพารามิเตอร์ ในด้านการจัดการควบคุมความปลอดภัยเครือข่าย Tencent Cloud ยังได้สร้างมาตรฐานการจัดการความปลอดภัยเครือข่ายและระบบป้องกันเครือข่ายแบบหลายชั้นภายในองค์กร Tencent Cloud กำหนดมาตรฐานการควบคุมและป้องกันความปลอดภัยเครือข่าย ตลอดจนบทบาทและความรับผิดชอบที่เกี่ยวข้องอย่างชัดเจนผ่านระบบการจัดการและขั้นตอนการทำงาน เพื่อให้มั่นใจว่ากิจกรรมที่ดำเนินการบนเครือข่ายของ Tencent Cloud ดำเนินไปอย่างปลอดภัย ในเวลาเดียวกัน Tencent Cloud ได้ปรับใช้สถาปัตยกรรมความปลอดภัยเครือข่ายที่ครบถ้วน โดยใช้กลไกการป้องกันหลายชั้น เช่น ไฟร์วอลล์ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) การป้องกัน DDoS การแยกทางลอจิคัลของเครือข่ายและความปลอดภัยของแอปพลิเคชันเว็บ เพื่อตรวจจับ กรอง และบล็อกการรับส่งข้อมูลเครือข่ายที่เป็นอันตรายได้ทันที ปกป้องความปลอดภัยเครือข่ายของ Tencent Cloud นอกจากนี้ Tencent Cloud ใช้มาตรการต่างๆ เช่น การควบคุมสิทธิ์และการอนุมัติขั้นตอน เพื่อห้ามไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงทรัพยากรเครือข่ายภายใน ซึ่งรวมถึงเครื่องมือวิเคราะห์และตรวจสอบเครือข่าย
6.1	2.6.5.1-2.6.5.8	บริหารจัดการ การซิด ความสา มารขอ	บริหารจัดการซิดความ สามารถของระบบเทคโนโลยีสารสนเทศและระบบสารสนเทศ บบสาธารณูปโภค	ลูกค้าควรเฝ้าติดตามการใช้ทรัพยากรแบบอย่างต่อเนื่อง กำหนดซิดจำกัดประสิทธิภาพและความจุ และดำเนินการกระบวนการที่จำเป็นเพื่อจัดการกับสถานการณ์ที่เกินซิดจำกัดที่กำหนดไว้ล่วงหน้า

ลำดับที่		โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
2	เทคโนโลยีสารสนเทศ	ระบบเทคโนโลยีสารสนเทศและระบบสารสนเทศ	(capacity management) เช่น การประเมินแนวโน้มการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศได้อย่างเพียงพอรองรับการให้บริการหรือดำเนินธุรกิจ และสามารถวางแผนการจัดการเทคโนโลยีสารสนเทศให้รองรับการใช้งานในอนาคต สำหรับระบบที่มีการให้บริการผ่านช่องทางดิจิทัลควรมีการติดตามและประเมินขีดความสามารถของระบบอย่างใกล้ชิด รองรับบริการและปริมาณธุรกรรมที่เพิ่มขึ้นอย่างรวดเร็ว	เพื่อสนับสนุนลูกค้าในการวางแผนและปรับขนาดความจุอย่างสะดวก Tencent Cloud ให้บริการ Auto Scaling (AS) สามารถตรวจสอบสถานะสุขภาพของอินสแตนซ์โดยอัตโนมัติ และปรับทรัพยากรการคำนวณของเซิร์ฟเวอร์คลาวด์โดยอัตโนมัติตามความต้องการทางธุรกิจ นโยบายและเงื่อนไขการขยายและลดขนาดที่กำหนดไว้ล่วงหน้าของลูกค้า เพื่อให้แน่ใจว่ามีอินสแตนซ์เซิร์ฟเวอร์คลาวด์ที่เพียงพอเสมอในการประมวลผลโหลดของแอปพลิเคชันของลูกค้า เพื่อให้บรรลุการตรวจสอบและจัดการประสิทธิภาพของระบบ ลูกค้าสามารถใช้ Tencent Cloud Observability Platform (TCOP) ซึ่งให้บริการตรวจสอบแบบเรียลไทม์ การวิเคราะห์ และการแจ้งเตือนสำหรับผลิตภัณฑ์/ทรัพยากรคลาวด์ รวบรวมและแสดงตัวชี้วัดการตรวจสอบต่างๆ ที่รายงานโดยผลิตภัณฑ์คลาวด์ เช่น เซิร์ฟเวอร์คลาวด์และฐานข้อมูลคลาวด์ รวมถึงตัวชี้วัดการตรวจสอบที่กำหนดเองและรายงานโดยลูกค้าผ่านแผนภูมิที่มองเห็นได้ ช่วยให้ลูกค้าติดตามอัตราการใช้ทรัพยากรผลิตภัณฑ์คลาวด์ ประสิทธิภาพของแอปพลิเคชัน และสถานะการทำงานของผลิตภัณฑ์คลาวด์แบบเรียลไทม์ และสนับสนุนการตั้งค่าการแจ้งเตือนตามตัวชี้วัด โดยแจ้งให้ลูกค้าทราบถึงความผิดปกติของธุรกิจอย่างทันทางที่ผ่านการส่งข้อความและช่องทางอื่นๆ ตามกฎการแจ้งเตือนที่ตั้งไว้ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ทำการคาดการณ์ความต้องการด้านความจุตามความต้องการในการดำเนินงานทางธุรกิจ และจัดทำแผนการจัดการความจุประจำปี ฝ่ายธุรกิจในขณะที่รับประกันความต่อเนื่องทางธุรกิจของระบบสารสนเทศ อ้างอิงแนวโน้มการใช้ความจุที่ได้รับจากการตรวจสอบก่อนหน้าและคำนึงถึงความต้องการของธุรกิจและระบบใหม่ ทำการคาดการณ์ความจุและวางแผนความจุ

ลำดับที่		โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			ในกระบวนการดำเนินงานประจำวัน ทีมงานภายใน Tencent Cloud ตรวจสอบการใช้ความจุของบริการสนับสนุนพื้นฐานของแพลตฟอร์มคลาวด์แบบเรียลไทม์ผ่านแพลตฟอร์มตรวจสอบความจุภายใน และระบุแนวโน้มการใช้ความจุเมื่อการใช้เกินขีดจำกัดที่กำหนดไว้ แพลตฟอร์มตรวจสอบจะแจ้งเตือนทีมงานที่เกี่ยวข้องให้ติดตามและดำเนินการที่เหมาะสม เพื่อให้แน่ใจว่าผลิตภัณฑ์และบริการทำงานอย่างราบรื่น
6.2	2.6.9.1-2.6.9.4	รักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน	ของผู้ใช้เทคโนโลยีสารสนเทศ (endpoint) ให้สามารถป้องกันการโจมตีด้วยรูปแบบต่างๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) รวมทั้งติดตามให้มีการปรับปรุงให้เป็นปัจจุบัน และหาทันภัยคุกคามใหม่ อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตี และป้องกันการรั่วไหลของข้อมูลหรือการเข้าใช้งานโดยไม่ได้รับอนุญาต	ลูกค้าควรใช้มาตรการป้องกันบนอุปกรณ์ปลายทาง โดยปรับใช้ซอฟต์แวร์ป้องกันไวรัสเพื่อสแกนระบบเป็นประจำ และอัปเดตฐานข้อมูลไวรัสอย่างทันทางที่ เพื่อให้สามารถเฝ้าระวังและระบุกิจกรรมที่ผิดปกติในระบบปลายทาง ลูกค้าสามารถใช้ Cloud Workload Protection Platform (CWPP) ใช้ข้อมูลภัยคุกคามจำนวนมหาศาลที่รวบรวมสะสมมาโดยใช้การเรียนรู้ของเครื่อง (Machine Learning) เพื่อให้บริการป้องกันความปลอดภัยแก่ลูกค้า เช่น การตรวจจับการบุกรุกของแฮกเกอร์ การแจ้งเตือนความเสี่ยงจากช่องโหว่ รวมถึงฟังก์ชันความปลอดภัยต่างๆ เช่น การบล็อกการถอดรหัสสแปม การแจ้งเตือนการเข้าสู่ระบบที่ผิดปกติ การตรวจจับไฟล์มัลแวร์โทรจัน การตรวจจับช่องโหว่ที่มีความเสี่ยงสูง เพื่อแก้ไขความเสี่ยงด้านความปลอดภัยเครือข่ายหลักที่เซิร์ฟเวอร์กำลังเผชิญอยู่ในปัจจุบัน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการป้องกันอุปกรณ์ปลายทางของโฮสต์ Tencent Cloud ได้ปรับใช้เครื่องมือตรวจจับและตอบสนองจุดปลายทาง (EDR) เพื่อตรวจสอบและควบคุมสินทรัพย์อุปกรณ์ปลายทางของเซิร์ฟเวอร์ทั่วทั้งเครือข่ายอย่างครอบคลุม เครื่องมือ EDR ที่ Tencent Cloud ใช้สนับสนุนการป้องกันไวรัสและการตรวจจับการบุกรุกเส้นฐานความปลอดภัยและการสแกนช่องโหว่

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโณโลยีสารสนเทศ			รวมถึงการตรวจสอบความสอดคล้องด้านความปลอดภัยสำหรับการดำเนินการคำสั่งและพฤติกรรมการเข้าสู่ระบบ และจะทริกเกอร์การแจ้งเตือนเมื่อตรวจพบโปรแกรมที่เป็นอันตรายหรือพฤติกรรมที่ผิดปกติ Tencent Cloud ติดตามและจัดการเหตุการณ์แจ้งเตือนผ่านระบบในงาน ในด้านการป้องกันอุปกรณ์ปลายทางในที่ทำงาน Tencent Cloud ได้กำหนดมาตรฐานความปลอดภัยของซอฟต์แวร์ภายในองค์กร ซึ่งกำหนดขีดจำกัดในการใช้ซอฟต์แวร์รับอุปกรณ์ปลายทางในที่ทำงาน (รวมถึงแล็ปท็อปและเวิร์กสเตชัน) และใช้เทคโนโลยีไวรัสสแตอปพลิเคชัน อนุญาตให้รันเฉพาะโปรแกรมที่รู้จักและเชื่อถือได้เท่านั้น เพื่อลดความเสี่ยงจากการบุกรุกของซอฟต์แวร์ที่เป็นอันตราย Tencent Cloud ยังควบคุมอุปกรณ์ปลายทางผ่านระบบจัดการความปลอดภัยแบบ Zero-Trust โดยใช้ความสามารถด้านความปลอดภัย เช่น การกำจัดไวรัส การแก้ไขช่องโหว่ และการป้องกันเชิงรุก เพื่อให้บรรลุการป้องกันความปลอดภัยรอบด้าน เช่น การป้องกันแรนซัมแวร์ การป้องกันการฟิชซิง การป้องกันการเคลื่อนย้ายภายใน เป็นต้น
6.3	2.6.8.1-2.6.8.5	สำรองข้อมูล	สำรองข้อมูล (data backup) ด้วยวิธีการและระยะเวลาที่เหมาะสม เช่น การสำรองข้อมูลประจำวัน เพื่อให้มีข้อมูลสำรองที่มีความพร้อมใช้งานในกรณีที่ระบบและข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย	ลูกค้าควรสร้างกลไกการจัดการการสำรองข้อมูล ทำการสำรองข้อมูลตามความถี่ที่กำหนด และดำเนินการทดสอบการกู้คืนจากการสำรองข้อมูลเป็นประจำ ภายในปี 2026 Tencent Cloud ได้ติดตั้งศูนย์ข้อมูลสามแห่งภายในประเทศไทย โดยแต่ละแห่งมีระบบไฟฟ้าและเครือข่ายที่ทำงานอิสระต่อกัน สามารถสนับสนุนให้ลูกค้าเก็บข้อมูล ประมวลผล และสำรองข้อมูลภายในประเทศได้ บริการจัดเก็บข้อมูลและบริการฐานข้อมูลหลายรายการที่ Tencent Cloud มอบให้ มีฟังก์ชันการสำรองข้อมูล พร้อมตอบสนองความต้องการสำรองข้อมูลทุกรูปแบบของลูกค้า ตัวอย่างเช่น:

ลำดับที่		โดเมน การคว การคว บคุม	ข้อกำหนดความค เฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโณโลยีสารสนเทศ			- ข้อมูลที่ถูกค่าเก็บไว้ใน <u>Cloud Object Storage (COS)</u> สามารถจัดเก็บข้อมูลในหลายพื้นที่ที่กำหนดพร้อมกันผ่านฟังก์ชันการทำสำเนาข้ามพื้นที่เพื่อให้แน่ใจว่าแม้ในกรณีที่สูญเสข้อมูลบางส่วนไปโดยไม่ได้คาดหมาย ก็ยังสามารถค้นหาและกู้คืนข้อมูลทั้งหมดได้ผ่านข้อมูลสำรอง และยังหลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้นเมื่อพื้นที่เก็บข้อมูลในโซนความพร้อมใช้งานหนึ่งประสบภัยพิบัติที่ไม่อาจหลีกเลี่ยงได้ ซึ่งช่วยให้บรรลุผลสำรองข้อมูลหลายชุดและการกู้คืนจากภัยพิบัติข้ามพื้นที่ - ฟังก์ชันการสำรองข้อมูลแบบสแนปช็อตของ <u>Cloud Block Storage (CBS)</u> ทำการสำรองข้อมูลโดยการถ่ายสแนปช็อต ณ จุดเวลาใดเวลาหนึ่งของ CBS ป้องกันการสูญเสข้อมูลเนื่องจากการแก้ไขโดยไม่ได้รับอนุญาตและการลบผิดพลาด และรับประกันความสามารถในการย้อนกลับอย่างรวดเร็วเมื่อเกิดความขัดข้องทางธุรกิจ <u>Cloud File Storage (CFS)</u> ให้ฟังก์ชันสแนปช็อตเป็นระยะ เพื่อความสะดวกในการตั้งค่านโยบายงานสำรองข้อมูลตามความยืดหยุ่นของลูกค้า <u>Cloud Native Database TDSQL-C</u> รองรับการสำรองข้อมูลสองประเภท: การสำรองข้อมูลเชิงตรรกะและการสำรองข้อมูลแบบสแนปช็อต ด้วยการสำรองข้อมูลที่สมบูรณ์และการสำรองข้อมูล binlog ในช่วงเวลาต่อมา ทำให้สามารถกู้คืนคลัสเตอร์ TDSQL-C MySQL Edition ทั้งหมดหรือตารางฐานข้อมูลเฉพาะไปยังจุดเวลาใดก็ได้ <u>TencentDB for MySQL</u> รองรับสองวิธีในการสำรองข้อมูลฐานข้อมูล: การสำรองข้อมูลอัตโนมัติและการสำรองข้อมูลด้วย

ลำดับที่		โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			ยตนเอง และให้ฟังก์ชันการสำรองข้อมูลข้ามพื้นที่เพื่อช่วยลูกค้าเพิ่มความสามารถในการกู้คืนจากภัยพิบัติและเพิ่มความน่าเชื่อถือของข้อมูลไปพร้อมๆ กัน TencentDB for MongoDB ให้กลไกการสำรองข้อมูลอัตโนมัติและการกู้คืนไบนารีไม่สูญเสียข้อมูล รองรับการสำรองข้อมูลแบบหลายโหนด ลูกค้าสามารถเก็บข้อมูลสำรองไว้หลายวันผ่านกลไกการสำรองข้อมูล เพื่อความสะดวกในการกู้คืนข้อมูลในสถานการณ์ภัยพิบัติ
6.4	2.6.4.1-2.6.4.4	จัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) ของเครื่องแม่ข่ายระบบงาน และอุปกรณ์เครือข่ายที่สำคัญ เช่น การจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (access log) และบันทึกการดำเนินงาน (activity log) เพื่อให้สามารถติดตามและตรวจสอบการเข้าถึงและการทำงานของระบบหรือข้อมูลและใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ได้ตามที่กฎหมายกำหนด		กค่าควรสร้างกลไกการจัดการบันทึก (log) เพื่อรวบรวม ประมวลผล และวิเคราะห์บันทึกของเซิร์ฟเวอร์ แอปพลิเคชัน และอุปกรณ์เครือข่ายที่สำคัญ และระบุพฤติกรรมที่น่าสงสัยหรือผิดปกติ เพื่อช่วยลูกค้าในกระบวนการรวบรวม สรุปและวิเคราะห์บันทึก Tencent Cloud ให้บริการ Cloud Log Service (CLS) ซึ่งเป็นแพลตฟอร์มบริการบันทึกแบบครบวงจร CLS ให้บริการหลายรายการตั้งแต่การรวบรวมบันทึกการจัดเก็บบันทึก ไปจนถึงการสืบค้นและวิเคราะห์บันทึก การบริโภคแบบเรียลไทม์ และการส่งบันทึก ช่วยลูกค้าแก้ไขปัญหาต่างๆ เช่น การดำเนินงานทางธุรกิจ การตรวจสอบความปลอดภัย การตรวจสอบบันทึก และการวิเคราะห์บันทึก CLS ออกแบบด้วยสถาปัตยกรรมแบบกระจายที่มีความพร้อมใช้งานสูง จัดเก็บข้อมูลบันทึกด้วยการสำรองข้อมูลหลายชุด ป้องกันไม่ให้ข้อมูลไม่สามารถใช้งานได้เมื่อบริการไหนขัดข้องล้มเหลว บรรลุความพร้อมใช้งานสูงของบริการ และให้การรับประกันบริการที่เสถียรและเชื่อถือได้สำหรับข้อมูลบันทึก Cloud Security Center (CSC) ยังสนับสนุนการรวบรวมข้อมูลที่เกี่ยวข้องกับความปลอดภัยบนคลาวด์ประเภทต่างๆ เช่น ข้อมูลการแจ้งเตือนของผลิตภัณฑ์ความปลอดภัยคลา

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโณโลยีสารสนเทศ			วดี ข้อมูลการเปลี่ยนแปลงการกำหนดค่าสินทรัพย์คลาวด์ ข้อมูลพฤติกรรมกรรมการดำเนินการของผู้ใช้บนคลาวด์ และข้อมูลบันทึกของผลิตภัณฑ์คลาวด์บางส่วน และให้แพลตฟอร์มการสืบค้นและสอบสวนแบบครบวงจร ช่วยลูกค้าบรรลุการตรวจสอบบันทึกและการสืบค้นและ สอบสวนบันทึกบนคลาวด์อย่างครอบคลุม นอกจากนี้ บริการ Elasticsearch Service (ES) จะรวบรวมและส่งบันทึกแบบเรียลไทม์ของเซิร์ฟเวอร์คล าวด์ คอนเทนเนอร์ และผลิตภัณฑ์คลาวด์อื่นๆ หรือข้อมูลธุรกิจที่มีอยู่และเพิ่มขึ้นของธุรกิจ ไปยังคลัสเตอร์ ES ของ Tencent Cloud เพื่อจัดเก็บข้อมูลแบบกระจาย และการสืบค้นและการวิเคราะห์ข้อมูล สำหรับการรวบรวมและการเก็บรักษาบันทึกเครือ ข่าย Cloud Firewall (CFW) รองรับการวิเคราะห์บันทึกเครือข่ายของปริมาณข้อมูล ทั้งหมด และสามารถเก็บรักษาได้สูงสุด 6 เดือน และรองรับการวิเคราะห์การติดตามภัยคุกคามขั้นสูง ซึ่งสามารถวิเคราะห์ข้อมูลการจดทะเบียนโดเมน การแก้ไข การขึ้นทะเบียน และประวัติการแก้ไขได้ สำหรับการรวบรวมและการเก็บรักษาบันทึกการ ดำเนินการ ลูกค้าสามารถใช้ CloudAudit เพื่อกำกับดูแลกิจกรรมบัญชี Tencent Cloud ตรวจสอบความสอดคล้อง ตรวจสอบการดำเนินการ และตรวจสอบความเสี่ยง CloudAudit รองรับการดูบันทึกการดำเนินการของคอนโซล Tencent Cloud และ API คลาวด์ภายใน 90 วันออนไลน์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการก ำกับดูแล ในด้านการจัดการบันทึก Tencent Cloud ได้สร้างมาตรฐานและกลไกการรวบรวมและการจัดการ บันทึก เพื่อควบคุมการบันทึก การดึงข้อมูล การจัดเก็บ การป้องกัน การวิเคราะห์ และการตรวจสอบบันทึกต่างๆ เช่น บันทึกการเข้าสู่ระบบ บันทึกการดำเนินการ บันทึกระบบทั่วไป

ลำดับที่		โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
2	2			และบันทึกเหตุการณ์ความผิดปกติของระบบเพื่อตรวจจับและป้องกันความผิดปกติและความเสี่ยงของกิจกรรมระบบ บันทึกทั้งหมดถูกรวมเข้าสู่แพลตฟอร์มการจัดการบันทึกของ Tencent Cloud เพื่อการจัดการ และมีการใช้มาตรการสำรองข้อมูลและการป้องกันที่เข้มงวดสำหรับข้อมูลบันทึกที่เกี่ยวข้อง เพื่อป้องกันการแก้ไขและการลบโดยไม่ได้รับอนุญาต Tencent Cloud ดำเนินการตรวจสอบบันทึกผ่านเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติการและทีมตรวจสอบภายใน เพื่อตรวจจับความผิดปกติของระบบหรือการดำเนินการ เพื่อป้องกันความเสี่ยงในการปฏิบัติการ
6.5	2.6.6.1-2.6.6.7	ติดตามดูและระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือสำหรับติดตามภัยคุกคามใหม่ ๆ และตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันที่	ติดตามดูและระบบและเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือสำหรับติดตามภัยคุกคามใหม่ ๆ และตรวจจับเหตุการณ์ผิดปกติหรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ เพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติและภัยคุกคามได้อย่างทันที่	ลูกค้าควรสร้างความสามารถในการรับรู้สถานการณ์ความปลอดภัยทางไซเบอร์ เพื่อเฝ้าระวังภัยคุกคามที่เกิดขึ้นใหม่ และตรวจจับเหตุการณ์ผิดปกติและภัยคุกคามที่มีผลกระทบต่อระบบสำคัญ เพื่อให้มั่นใจในการค้นพบ การป้องกัน และการตอบสนองได้ทันที่ เพื่อสนับสนุนลูกค้าในการตรวจจับและวิเคราะห์ภัยคุกคาม Tencent Cloud ให้บริการ Threat Intelligence X (TIX) แก่ลูกค้า ซึ่งเป็นแพลตฟอร์มบริการข่าวกรองแบบครบวงจร TIX สามารถให้ความสามารถด้านข่าวกรองสามประเภทหลัก ได้แก่ ข่าวกรองพื้นฐาน ข่าวกรองด้านพื้นผิวการโจมตี และข่าวกรองทางธุรกิจรองรับฟังก์ชันต่างๆ เช่น การสืบค้นข่าวกรองการวิเคราะห์และประเมิน IOC การจัดการพื้นผิวการโจมตี สามารถช่วยลูกค้าวิเคราะห์และประเมินเหตุการณ์ความผิดปกติได้อย่างมีประสิทธิภาพมากขึ้น และประเมินความเสี่ยงด้านการเปิดเผยสินทรัพย์ขององค์กรอย่างครอบคลุมมากขึ้น สนับสนุนองค์กรในการสร้างระบบป้องกันความปลอดภัยแบบสามมิติที่มีประสิทธิภาพ TIX สร้างเครือข่ายจุดสัมผัสข่าวกรองที่สมบูรณ์ โดยรวบรวมและวิเคราะห์ข่าวกรองภัยคุกคามจากแหล่งที่มาหลากหลาย เช่น ชุมชนช่องโหว่

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโณโลยีสารสนเทศ			องค์กรความปลอดภัย ผู้ผลิตเครื่องมือความปลอดภัย โซเชียลมีเดีย บล็อกความปลอดภัย และเชื่อมโยงกับอัลกอริธึมและพลังการคำนวณบนคลาวด์เพื่อจัดผลบวกปลอม ซึ่งรับประกันความแม่นยำของข่าวกรอง นอกจากนี้ ศูนย์ข่าวกรองภัยคุกคามใช้ SaaS เป็นแกนกลาง รองรับวิธีการส่งมอบต่างๆ เช่น API ฝั่งเว็บ SDK TIP และ Mini Program เพื่อตอบสนองความต้องการที่หลากหลายของลูกค้า ศูนย์ข่าวกรองภัยคุกคามยังสามารถบูรณาการกับผลิตภัณฑ์ป้องกันความปลอดภัยที่มีอยู่ของลูกค้าในรูปแบบการรวมเข้าด้วยกัน เพื่อเชื่อมโยงข้อมูลข่าวกรองจากคลาวด์กับผลิตภัณฑ์ดังกล่าว เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัยโดยรวมและการตอบสนองต่อภัยคุกคาม ด้วยการเสริมพลังและการสนับสนุนจากศูนย์ข่าวกรองภัยคุกคาม Tencent Cloud มุ่งมั่นที่จะสร้างระบบความสามารถด้านความปลอดภัยในการป้องกันเชิงรุกแบบ "ข่าวกรอง-การโจมตีและการป้องกัน-การจัดการ-การวางแผน" โดยบูรณาการเทคโนโลยีต่างๆ เช่น ข่าวกรองภัยคุกคาม ปัญญาประดิษฐ์ ข้อมูลขนาดใหญ่ เพื่อเพิ่มความสามารถและประสิทธิภาพในการตอบสนองต่อเหตุการณ์ความปลอดภัย และได้จัดตั้งศูนย์ปฏิบัติการความปลอดภัยที่ทำงาน 24 ชั่วโมงทุกวัน ให้ความสำคัญกับการตรวจจับภัยคุกคาม การสอบสวน และการตอบสนอง เพื่อให้บรรลุความสามารถในการรับรู้ มองเห็น และควบคุมสถานการณ์ความปลอดภัย
6.6	2.6.7.1-2.6.7.7	บริหารจัดการช่องโหว่	บริหารจัดการช่องโหว่ (vulnerability management) โดยจัดให้มีการประเมินช่องโหว่สำหรับทุกระบบงานตามระดับความเสี่ยงสำหรับระบบงานสำคัญที่ต้องดำเนินการอย่าง	ลูกค้าควรดำเนินการประเมินช่องโหว่และการทดสอบเจาะระบบเป็นประจำ เพื่อระบุช่องโหว่ด้านความปลอดภัยและประเมินความสามารถในการป้องกันความปลอดภัยทางไซเบอร์ของตน ในด้านการทดสอบเจาะระบบ Tencent Cloud ให้บริการ Penetration Testing Service (PTS) แก่ลูกค้า ด้วยการจำลองเทคนิคการโจมตีและเทคนิคการค้นพบ

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ หารความเสี่ยงด้านเท ค			
2	ค	นโ	ยปีละ 1 ครั้ง และ เมื่อมีการเปลี่ยนแปลง อย่างมีนัยสำคัญ	ช่องโหว่ที่แฮกเกอร์อาจใช้อย่างเต็มรูปแบบ ใช้วิธีการและกลไกที่ควบคุมได้และไม่ทำลายล้างเพื่อทำ การตรวจสอบความปลอดภัยของระบบเป้าหมายอย่างลึก ซึ้ง
6.7	2.6.7.1-2.6.7.7	ทดสอบเ จาระบบ	ทดสอบเจาะระบบ (penetration test) โดยจัดให้มีการทดสอบ เจาะระบบ โดยผู้เชี่ยวชาญภายใน หรือภายนอกที่มีความ เป็นอิสระ อย่างน้อยครอบคลุมระ บบงานและระบบเครือข าย ที่มีการเชื่อมต่อกับเคร ือข่ายสื่อสารสาธารณะ (Internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และ เมื่อมีการเปลี่ยนแปลง อย่างมีนัยสำคัญ	ค้นหาจุดอ่อนที่มีอยู่ในเป้าหมายและอุปกรณ์เครือข่าย ให้คำแนะนำในการเสริมความแข็งแกร่งด้านความปลอด ภัยเพื่อช่วยลูกค้ายกระดับความปลอดภัยของระบบ และสนับสนุนการตรวจสอบหลังการแก้ไขช่องโหว่ ในด้านการสแกนช่องโหว่ ลูกค้าสามารถเลือกใช้ <u>Vulnerability Scanning Service (VSS)</u> เพื่อตรวจสอบสินทรัพย์เครือข่ายขององค์กรและระบุคว ามเสี่ยงของสินทรัพย์นั้นๆ โดยใช้ประโยชน์จากประสบการณ์ด้านความปลอดภัยและ ผู้เชี่ยวชาญคุณภาพที่สะสมมาหลายปีของ Tencent Cloud VSS ได้สร้างฐานข้อมูลกฎช่องโหว่ที่อุดมสมบูรณ์และครอบคลุม และมีความสามารถในการตรวจจับช่องโหว่ 0Day/1Day/NDay ที่มีอาชัฟและมีประสิทธิภาพสูง สามารถดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของสินทรัพย์ของลูกค้า ให้คำแนะนำการแก้ไขที่มีอาชัฟแก่ลูกค้า เพื่อลดความเสี่ยงด้านความปลอดภัย VSS ยังสนับสนุนการทำงานร่วมกับผลิตภัณฑ์คลาวด์ เช่น ความปลอดภัยโฮสต์ไฟร์วอลล์แอปพลิเคชันเว็บ เพื่อให้บรรลุวงจรปิดจากการตรวจสอบความเสี่ยงไปจนถึง การจัดการความเสี่ยง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการก กับดูแล Tencent Cloud จะสร้างงานสแกนเป็นประจำผ่านระบบสแกนช่องโหว่เพื่ อสแกนช่องโหว่ของสินทรัพย์ในสภาพแวดล้อมคลาวด์ และวิเคราะห์ จัดประเภท และดำเนินการแก้ไขช่องโหว่ที่พบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะดำเนินการทดสอบเจาะระบบขนาดใหญ่แบบเต็มวงจ รเป็นประจำ และดำเนินการทดสอบเจาะระบบแบบเจาะจงอย่างยืดห

ลำดับที่		โดเมน การคว มคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ หารแบบ			
2	ความปลอดภัยด้านเทค นอลยีสารสนเทศ			อยู่ในสถานการณ์ต่างๆ เช่น ก่อนการเปิดตัวผลิตภัณฑ์ใหม่หรือเมื่อมีการเปลี่ยนแปลงครั้งสำคัญ ผลการทดสอบเจาะระบบจะแจ้งให้ฝ่ายงานผู้รับผิดชอบที่เกี่ยวข้องทราบผ่านใบงานความปลอดภัย และฝ่ายงานผู้รับผิดชอบจะดำเนินการปะชองโหวหรือดำเนินการมาตรการควบคุมชดเชยอื่นๆ ทันที เพื่อให้มั่นใจว่าช่องโหว่ที่โซ่ประโยชน์ได้ซึ่งพบในการทดสอบเจาะระบบได้รับการจัดการอย่างเหมาะสม นอกจากนี้ Tencent Cloud ยังดำเนินการฝึกซ้อมการต่อสู้เสมือนระหว่างทีมแดงและทีมน้ำเงินเพื่อจำลองการต้านทานการโจมตีทางเครือข่ายเป็นประจำ Tencent Cloud ยังได้สร้างแพลตฟอร์มรับข้อเสนอแนะช่องโหว่จากภายนอกและดำเนิน "โครงการให้รางวัลการรายงานช่องโหว่" โดยเชิญผู้เชี่ยวชาญด้านความปลอดภัยในอุตสาหกรรมช่วย Tencent Cloud ค้นพบช่องโหว่และความเสี่ยงด้านความปลอดภัยของระบบจากมุมมองของแฮกเกอร์ เพื่อแก้ไขปัญหาด้านความปลอดภัยได้ทันทั่วทั้ง และบำรุงรักษาความปลอดภัยของระบบนิเวศของ Tencent Cloud
6.8	2.6.1.1- 2.6.1.10	บริหารจัดการการเปลี่ยนแปลง	บริหารจัดการการเปลี่ยนแปลง (change management) โดยจัดให้มีกระบวนการบริหารจัดการการเปลี่ยนแปลงและควบคุมการเปลี่ยนแปลงอย่างรัดกุมและเพียงพอ เช่น การนำระบบขึ้นใช้งานจริง (system deployment) การตั้งค่าระบบ (system configuration)	ลูกค้าควรกำหนดขั้นตอนการจัดการการเปลี่ยนแปลงโดยการเปลี่ยนแปลงทุกประเภทควรได้รับการประเมินทดสอบ ทบทวน และอนุมัติก่อนการดำเนินการ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานการจัดการสำหรับการเปลี่ยนแปลงผลิตภัณฑ์และการกำหนดค่าที่กำหนดขั้นตอนต่างๆ ในกระบวนการเปลี่ยนแปลงและผู้รับผิดชอบที่เกี่ยวข้องอย่างชัดเจน เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการอนุมัติและทดสอบอย่างเหมาะสมก่อนการดำเนินการ ในเวลาเดียวกัน Tencent Cloud ได้กำหนดขั้นตอนการจัดการสำหรับการเปลี่ยนแปลงฉุกเฉิน โดยการเปลี่ยนแปลงฉุกเฉินต้องได้รับการอนุมัติที่เหมาะสม

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ รณ			
2	ความปลอดภัยด้านเท คโนโลยีสารสนเทศ		การติดตั้ง patch เพื่อให้ การเปลี่ยนแปลงเป็นไป ตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบ ถ้วน และป้องกันการเปลี่ยนแปลง โดยไม่ได้รับอนุญาต	จะสามารถดำเนินการได้ การเปลี่ยนแปลงโปรแกรมทุกประเภท รวมถึงการเปลี่ยนแปลงแอปพลิเคชันและไฟล์กำหนดค า ระบบปฏิบัติการ และฐานข้อมูล ต้องได้รับการวิเคราะห์ผลกระทบทางธุรกิจก่อนการเปิด ตัว จัดทำแผนย้อนกลับสำหรับการเปลี่ยนแปลง และได้รับการอนุมัติจากผู้รับผิดชอบที่เกี่ยวข้อง ระบบเผยแพร่การเปลี่ยนแปลงของ Tencent Cloud บังคับให้การดำเนินการเปลี่ยนแปลงสามารถดำเนินการ ได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น และเก็บรักษาบันทึกที่เกี่ยวข้องกับการเปลี่ยนแปลงไว้ พร้อมทั้งตรวจสอบบันทึกเป็นประจำ หลังการเผยแพร่การเปลี่ยนแปลง Tencent Cloud จะตรวจสอบ ตรวจสอบ และบันทึกผลการเปลี่ยนแปลงในสภาพแวดล้อมการผลิต Tencent Cloud จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอการ ดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน และขอบเขตของการเปลี่ยนแปลง สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแ วล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขยาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม
6.9	2.6.2.1-2.6.2.4	บริหารจั ดการการ ตั้งค่าระบบ	บริหารจัดการการตั้งค่า ระบบ (system configuration management) โดยจัดให้มี การกำหนดมาตรฐาน การรักษาความมั่นคงป ลอดภัยขั้นต่ำ (minimum security baseline) และกระบวนการตั้งค่า การรักษาความมั่นคงป	ลูกค้าควรกำหนดมาตรฐานความปลอดภัยสำหรับซอฟต์แวร์และฮาร์ดแวร์ที่สนับสนุนระบบสำคัญ ดำเนินการกำหนดค่าความปลอดภัย และสร้างกระบวนการที่เกี่ยวข้องเพื่อตรวจสอบความเป็ ยงเบนของการกำหนดค่าในระบบจากมาตรฐานความป ลอดภัย Cloud Security Center (CSC) ให้ฟังก์ชันการตรวจสอบและประเมินความเสี่ยงการกำ หนดค่าผลิตภัณฑ์คลาวด์โดยอัตโนมัติ ช่วยลูกค้าลดความเสี่ยงด้านความปลอดภัยที่เกิดจาก ข้อผิดพลาดในการกำหนดค่าความปลอดภัยในการใช้

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโณโลยีสารสนเทศ		ลดภัยสลดคล่องกับม าตรฐานดังกล่าว (security hardening) ครอบคลุมระบบปฏิบัติ การ ระบบฐานข้อมูล ระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาควา มปลอดภัยเครือข่ายที่ รองรับระบบงาน สำคัญให้ชัดเจนเป็นลา ยลักษณะอักษร รวมทั้งดำเนินการตั้งค าและสอบทานการตั้งค าอย่างสม่ำเสมอตามที่ ได้กำหนดไว้ เพื่อให้มั่นใจว่าระบบงาน ที่รองรับการให้บริการ มีการรักษาความมั่น คงปลอดภัยขั้นต่ำตาม มาตรฐาน ที่กำหนดไว้ในกรณีทีส ถาบันการเงินหรือสกา บันการเงินเฉพาะกิจไม่ สามารถปฏิบัติตามมา ตรฐาน ที่ตนได้กำหนดไว้ข้างต้ น ต้องจัดให้มีกระบวนกา รขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยง และ พิจารณาแนวทางควบ คุมความเสี่ยงที่เพียงพอ เหมาะสมก่อนดำเนินการ	ผลิตภัณฑ์คลาวด์ และยกระดับความปลอดภัยโดยรวมบนคลาวด์ ในเวลาเดียวกัน ลูกค้าสามารถใช้ Config เพื่อดำเนินการตรวจสอบและควบคุมทรัพยากรคลาวด์ จากส่วนกลาง บันทึกข้อมูลการกำหนดค่าและการเปลี่ยนแปลงการกำหนดค่าของทรัพยากรคลาวด์ต่างๆ ในภูมิภาคต่างๆ ภายใต้บัญชีของลูกค้าอย่างต่อเนื่อง และอิงตามกฎข้อปฏิบัติที่ดีที่สุดและเหมาะสมเพื่อเคจ การปฏิบัติตามข้อกำหนดของ Tencent Cloud เพื่อประเมินความสอดคล้องของการกำหนดค่าทรัพยากรคลาวด์ภายใต้บัญชีองค์กรอย่างต่อเนื่องโดยอัตโนมัติ และระบุการกำหนดค่าทรัพยากรที่ไม่สอดคล้อง เพื่อให้บรรลุการตรวจสอบและจัดการทรัพยากรคลาวด์ โดยอัตโนมัติ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างระบบการจัดการการกำหนดค่า และบริหารจัดการส่วนประกอบบริการเทคโนโลยีสารสนเทศและรายการกำหนดค่าต่างๆ อย่างเป็นเอกภาพผ่านฐานข้อมูลการจัดการการกำหนดค่า รวมถึงควบคุมการจัดการรายการกำหนดค่า (CI) และความสัมพันธ์ระหว่างรายการดังกล่าว หากกระบวนการเปลี่ยนแปลงเกี่ยวข้องกับการอัปเดตการกำหนดค่า เจ้าหน้าที่ปฏิบัติการจะอัปเดตรุ่นและข้อมูลที่เกี่ยวข้องของรายการกำหนดค่าลงในฐานข้อมูลการจัดการการกำหนดค่าตามแผนการเปลี่ยนแปลง หลังจากดำเนินการเปลี่ยนแปลงเสร็จสิ้น Tencent Cloud จะตรวจนับสินทรัพย์เป็นประจำ และตรวจสอบฐานข้อมูลการจัดการการกำหนดค่า เพื่อให้มั่นใจในประสิทธิภาพ ความถูกต้อง และความสมบูรณ์ของข้อมูลรายการกำหนดค่าต่างๆ เพื่อให้สอดคล้องกับข้อกำหนดการกำกับดูแลของลูกค้า ๆ Tencent Cloud ได้กำหนดมาตรฐานการกำหนดค่าความปลอดภัยเครือข่ายและมาตรฐานเส้นฐานความปลอดภัยขึ้น เพื่อจัดการมาตรฐานการกำหนดค่าความปลอดภัยของอุปกรณ์เครือข่าย ไฟร์วอลล์

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ รแบบ			
2	ความปลอดภัยด้านเท คโนโลยีสารสนเทศ			ระบบปฏิบัติการของเซิร์ฟเวอร์โฮสต์ ฐานข้อมูล และระบบแอปพลิเคชัน Tencent Cloud ใช้เครื่องมือสแกนเพื่อตรวจจับความเบี่ยงเบนของการกำหนดค่าระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และอิมเมจเสมือน (Virtual Image) จากมาตรฐานอย่างต่อเนื่อง สำหรับความเบี่ยงเบนที่ตรวจพบ Tencent Cloud จะสร้างใบงานความปลอดภัยและส่งไปยังทีมงานผู้รับผิดชอบโดยอัตโนมัติ เพื่อดำเนินการแก้ไขทันทีที่ Tencent Cloud ยังทบทวนนโยบายความปลอดภัยและการตั้งค่าพารามิเตอร์ของอุปกรณ์เครือข่าย เช่น เราเตอร์ ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย เป็นระยะ เพื่อให้มั่นใจในประสิทธิภาพของนโยบายและพารามิเตอร์
6.10	2.6.3.1-2.6.3.6	บริหารจัดการ ดการ patch	บริหารจัดการ patch (patch management) โดยต้องจัดให้มีกระบวนการ บริหารจัดการ security patch ในทุกระบบงานและอุปกรณ์ เพื่อเป็นการลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศจะถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่ และระดับความสำคัญของระบบงาน ในกรณีที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ	ลูกค้าควรสร้างกลไกการจัดการแพตช์ความปลอดภัย และปรับใช้แพตช์ความปลอดภัยตามระดับความรุนแรงของช่องโหว่และความสำคัญของระบบ ลูกค้ายังสามารถใช้ Cloud Workload Protection Platform (CWPP) เพื่อตรวจจับช่องโหว่ซอฟต์แวร์ Linux ช่องโหว่ระบบปฏิบัติการ Windows ช่องโหว่ Web-CMS และช่องโหว่แอปพลิเคชัน แจ้งเตือนแบบเรียลไทม์ และรับโซลูชันการแก้ไขช่องโหว่ ช่วยลูกค้าตอบสนองต่อความเสี่ยงจากช่องโหว่อย่างรวดเร็ว Tencent Container Security Service (TCSS) เป็นระบบแพตช์เสมือนที่ Tencent Cloud Security พัฒนาขึ้นเพื่อป้องกันช่องโหว่วันศูนย์ (zero-day) ที่เกิดขึ้นบ่อยครั้ง ซึ่งผสมรวมเทคโนโลยีการขุดเจาะช่องโหว่และการแจ้งเตือนช่องโหว่ร้ายแรงแบบเรียลไทม์ของ Tencent ใช้เพื่อตรวจจับและวิเคราะห์ช่องโหว่ สร้างแพตช์เสมือนตามความรู้ความเชี่ยวชาญของ Tencent และทำให้แพตช์เสมือนมีผลบนเซิร์ฟเวอร์คลาวด์โดยอัตโนมัติ เพื่อป้องกันการโจมตีของแฮกเกอร์ได้อย่างมีประสิทธิภาพ นอกจากนี้ ลูกค้ายังสามารถใช้ Vulnerability Scanning Service (VSS) เพื่อดำเนินการสแกนความปลอดภัยเป็นประจำ

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโนโยีสารสนเทศ		สถาบันการเงินและส ก าบันการเงินเฉพาะกิจ ต้องจัดให้มี การควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจาก การถูกโจมตีจากช่องโ หานั้น ๆ นอกจากนี้ กรณีที่ไม่สามารถติดต้ ง security patch ได้ ต้องจัดให้มีกระบวนกา ร ขออนุมัติยกเว้นและดำ เนินการประเมินความเม เสี่ยง รวมทั้งพิจารณาแนวท างควบคุมความเสี่ยงที่เ ียงพอเหมาะสม	การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของอุปกรณ์เครือข่ายและบริการแ อปพลิเคชันขององค์กร และใช้คำแนะนำการแก้ไขที่มีอาชีจาก VSS เพื่อลดความเสี่ยงด้านความปลอดภัยขององค์กร เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำ กับดูแล ในด้านการจัดการแพตช์ Tencent Cloud จะระบุแพตช์ล่าสุด และดำเนินการทดสอบความปลอดภัยอย่างเพียงพอก่อ นการติดตั้งแพตช์ เพื่อให้มั่นใจในความปลอดภัยของการติดตั้งแพตช์ Tencent Cloud จะแจ้งให้ทีมงานธุรกิจภายในแต่ละทีมทราบเป็นประจำ เกี่ยวกับการอัปเดตและติดตั้งแพตช์ และใช้เครื่องมือตรวจจับจุดปลายทาง (endpoint) สแกนสถานะการติดตั้งแพตช์เป็นประจำ และอุปกรณ์ที่ไม่ได้ติดตั้งแพตช์เกินกำหนดเวลาจะถูก สร้างใบงานแจ้งเตือนโดยอัตโนมัติ ในเวลาเดียวกัน Tencent Cloud ยังได้สร้างกลไกการสแกนช่องโหว่ภายในและแพลตฟอร์ม รวบรวมช่องโหว่ภายนอก เพื่อรายงานปัญหาช่องโหว่และภัยคุกคามทั้งภายในและ ภายนอก ใบงานช่องโหว่ความปลอดภัยจะถูกบันทึกไว้ในระบบปฏิ บัติการความปลอดภัยและถูกกำหนดให้ผู้รับผิดชอบที่เ กี่ยวข้องดำเนินการภายในเวลาที่กำหนด นอกจากนี้ ทีมวิจัยความปลอดภัยของ Tencent Cloud ได้พิสูจน์ความสามารถในการป้องกันช่องโหว่ลงในระบบ ไฟร์วอลล์แอปพลิเคชันเว็บของ Tencent Cloud ในรูปแบบแพตช์เสมือน เพื่อให้มั่นใจในความปลอดภัยโดยรวมของแพลตฟอร์ม คอมพิวเตอร์คลาวด์
7.1, 7.2	2.7.1, 2.7.2	การจัดห าและการ พัฒนาระ บบ	กำหนดหลักเกณฑ์ที่ช้ ดเจนและเหมาะสมในก ารคัดเลือกระบบและบุ คคลภายนอก ที่ให้บริการ เช่น	ลูกค้าควรกำหนดมาตรฐานและขั้นตอนสำหรับการจัด หาและการพัฒนาระบบ กำหนดข้อกำหนดด้านความปลอดภัยในกระบวนการอ อกแบบ พัฒนา และทดสอบระบบให้ชัดเจน เพื่อให้มั่นใจในความปลอดภัย ความน่าเชื่อถือ

ลำดับที่		โดเมน การคว มคุ้ม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คในโลยีสารสนเทศ		ความน่าเชื่อถือของระบบ บุคคลภายนอกที่ให้บริการที่รับการรับรองตามมาตรฐานสากลที่ได้รับ การยอมรับโดยทั่วไป (certificate) ความมั่นคงปลอดภัยของระบบ การสนับสนุนและการบำรุงรักษาระบบเป็นต้น เพื่อให้มั่นใจว่าระบบและบุคคลภายนอกที่ให้บริการสามารถตอบสนองต่อความต้องการในการดำเนินการได้ รวมถึงต้องคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการที่บุคคลภายนอก การเปลี่ยนแปลงเทคโนโลยีสารสนเทศ หรือการเปลี่ยนแปลงกลยุทธ์ในการให้บริการหรือดำเนินธุรกิจในอนาคตออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีการรักษาความลับของระบบและข้อมูล ความถูกต้องเชื่อถือได้พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอที่จะรองรับการปรับปรุง เปลี่ยนแปลงระบบในอนาคต	และความพร้อมใช้งานของระบบ สำหรับบริการพัฒนาระบบที่ได้รับจากซัพพลายเออร์หรือผู้พัฒนาภายนอก ควรตกลงความรับผิดชอบของทั้งสองฝ่ายผ่านข้อตกลงการซื้อขายหรือสัญญา เพื่อสนับสนุนลูกค้าในการจัดการวงจรชีวิตการพัฒนา Tencent Cloud ให้บริการเครื่องมือนักพัฒนา Cloud Native Build (CNB) CNB อิงตามระบบนิเวศ Docker ทำให้สิ่งแวดล้อม แคช และปลั๊กอินเป็นนามธรรม และใช้ไวยากรณ์เชิงประกาศ มีจุดมุ่งหมายเพื่อช่วยให้นักพัฒนาสร้างซอฟต์แวร์ด้วยวิธีที่มีประสิทธิภาพมากขึ้น CNB จัดเตรียมเซิร์ฟเวอร์เครื่องมือนักพัฒนาที่สมบูรณ์ มีความสามารถ เช่น การโฮสต์โค้ด ไปป์ไลน์การวิจัยและพัฒนาที่มีประสิทธิภาพสูง การตรวจสอบโค้ดด้วย AI สภาพแวดล้อมการพัฒนานบนคลาวด์ การจัดการอาร์ติแฟกต์ และชุดงานที่กำหนดเอง ซึ่งสามารถสนับสนุนกระบวนการวิจัยและพัฒนาตั้งแต่ความต้องการไปจนถึงการปรับใช้และการจัดการการพัฒนารวมถึงคล่องตัวได้อย่างมีประสิทธิภาพ เพื่อช่วยเหลือลูกค้าในการจัดการระบบของ Tencent Cloud Tencent Cloud ได้จัดเตรียมเอกสารกฎหมายออนไลน์ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement และอิงตามสถานการณ์จริงและความต้องการของลูกค้า เพื่อเจรจาตกลงเกี่ยวกับสิทธิ์การตรวจสอบและสิทธิ์การกำกับดูแลของลูกค้าในข้อตกลงกับลูกค้า สำหรับภาพรวมของ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ในด้านต่างๆ ของการตรวจสอบอย่างละเอียด โปรดดูเนื้อหาในข้อ "8 การคัดเลือกบุคคลภายนอก" ในบทที่ 5.7.2 ของ "5.7.2 การบริหารจัดการความเสี่ยงจากบุคคลภายนอก" ในคู่มือนี้ ในด้านการจัดการวงจรชีวิตการพัฒนาระบบควมปลอดภัย Tencent Cloud

ลำดับที่		โดเมน การคว มคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ หารแนว			
2	ความปลอดภัยด้านเท คโนโลยีสารสนเทศ			ยังได้สร้างมาตรฐานการพัฒนาความปลอดภัยระบบสารสนเทศภายในองค์กร และมุ่งมั่นผสานมาตรฐาน ISO/IEC 20000 การจัดการบริการเทคโนโลยีสารสนเทศ ระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001 และมาตรฐานระบบการจัดการคุณภาพ ISO/IEC 9001 เข้ากับกระบวนการวงจรชีวิตการพัฒนาความปลอดภัยผลิตภัณฑ์ทั้งหมด ให้มีความสำคัญกับขั้นตอนต่างๆ เช่น ความต้องการ การออกแบบ การวิจัยและพัฒนา การทดสอบ การส่งมอบ และการดำเนินการและบำรุงรักษา ผสานแนวคิดด้านความปลอดภัยข้อมูลและการปกป้องความเป็นส่วนตัวเข้าไปในแต่ละขั้นตอนของการพัฒนาผลิตภัณฑ์ เพื่อให้มั่นใจว่าผลิตภัณฑ์คลาวด์ได้รับความควบคุมด้านความปลอดภัยที่เพียงพอตลอดวงจรชีวิตของผลิตภัณฑ์ มาตรการควบคุมความปลอดภัยที่เกี่ยวข้อง ได้แก่: การฝึกอบรมความปลอดภัย: ส่งเสริมจิตสำนึกการเขียนโปรแกรมที่ปลอดภัยสำหรับนักพัฒนา กำหนดให้นักพัฒนาปฏิบัติตามมาตรฐานการเข้ารหัสที่ปลอดภัยอย่างเคร่งครัด การวิเคราะห์ความต้องการ: สื่อสารเกี่ยวกับเนื้อหาและกระบวนการธุรกิจและกรอบทางเทคนิค เพื่อค้นหาวิธีที่ดีที่สุดในการฝังความปลอดภัย การออกแบบระบบ: สร้างแบบจำลองภัยคุกคามสำหรับการออกแบบระบบ และประเมินความปลอดภัยทางเทคนิคของสถาปัตยกรรมที่ใช้ การพัฒนาระบบ: ในระหว่างกระบวนการพัฒนา จัดเตรียมส่วนประกอบการพัฒนาความปลอดภัยที่ Tencent ออกแบบเองสำหรับนักพัฒนาใช้ และเขียนโค้ดตามมาตรฐานการเข้ารหัสความปลอดภัย

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโนโลยีสารสนเทศ			อดภัยของ Tencent Cloud การยืนยันความปลอดภัย: ค้นพบช่องโหว่ผ่านการตรวจสอบความปลอดภัย ของโค้ด การสแกนความปลอดภัยของสินทรัพย์ การสแกนเว็บ การประเมินความปลอดภัยด้วยมนุษย์ การทดสอบเจาะระบบ และการตรวจสอบโค้ด การเผยแพร่: ระบบจะเผยแพร่ไปยังสภาพแวดล้อมออนไลน์ได้ก็ ต่อเมื่อความเสี่ยงสูงทั้งหมดได้รับการแก้ไขแล้ว เพื่อป้องกันไม่ให้เกิดผลกระทบทำงานในสภาพแวดล้อม ผลิตโดยมีช่องโหว่ด้านความปลอดภัย นอกจากนี้ Tencent Cloud รับรองว่าสภาพแวดล้อมการพัฒนา/ทดสอบและสภาพ แวดล้อมการผลิตถูกแยกออกจากกัน และห้ามใช้ข้อมูลการผลิตที่ยังไม่ได้ปิดในสภาพแวดล้อมการพัฒนา/ทดสอบ Tencent Cloud ยังได้กำหนดกลไกนโยบายการให้สิทธิ์และการแยกเมท ริกซ์สิทธิ์ในการควบคุมการเข้าถึงภายใน เพื่อรับรองการแยกหน้าที่ระหว่างบุคลากรที่เกี่ยวข้องกั บการพัฒนาซอฟต์แวร์ การทดสอบ และการเผยแพร่ สำหรับการใช้ผลิตภัณฑ์บุคคลที่สาม Tencent Cloud ได้กำหนดข้อกำหนดด้านการจัดการความปลอดภัยข องซัพพลายเชน โดยกำหนดให้ต้องมีการตรวจสอบการอนุญาตเข้าความ ปลอดภัยเมื่อนำเข้าองค์ประกอบภายนอก และจำเป็นต้องมีการเสริมความแข็งแกร่งด้านความปล อดภัยและการป้องกันก่อนการเปิดใช้งาน เพื่อให้มั่นใจว่าผลิตภัณฑ์ผ่านการตรวจสอบความปล อดภัยก่อนเปิดใช้งาน หลังผลิตภัณฑ์เปิดใช้งาน จะดำเนินการปฏิบัติการและบำรุงรักษาด้านความปล อดภัยและการตรวจสอบความปลอดภัยอย่างต่อเนื่อง เพื่อแก้ไขปัญหาด้านความปลอดภัยได้ทันทั่วทั้งที่ และผ่านการประเมินสถานการณ์การดำเนินงานด้านค วามปลอดภัยของผลิตภัณฑ์ เพื่อระบุความเสี่ยงด้านความปลอดภัยและกระตุ้นให้ซัพ พลายเออร์ปรับปรุง

ลำดับที่		โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
2				ตลอดจนทบทวนกลยุทธ์ความร่วมมือกับซัพพลายเออร์ดังกล่าวในอนาคต นอกจากนี้ Tencent Cloud ยังได้สร้างมาตรฐานการจัดการความปลอดภัยของส่วนประกอบโอเพนซอร์ส เพื่อให้มั่นใจว่าแหล่งที่มาของส่วนประกอบโอเพนซอร์สที่ทีมพัฒนานำเข้ามามีความน่าเชื่อถือ และผ่านการตรวจสอบความปลอดภัย เพื่อให้มั่นใจในความปลอดภัยและความถูกต้องตามกฎหมายในการใช้ส่วนประกอบโอเพนซอร์ส
8	2.8.1, 2.8.2	การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยบันทึกวิเคราะห์และรายงานเหตุการณ์ผิดปกติ ปัญหา และการแก้ไขให้คณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายกรณีเป็นสาขานาการพาณิชย์ ต่างประเทศ ในระยะเวลาที่เหมาะสม นอกจากนี้ ต้องวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต	บริหารจัดการเหตุการณ์ผิดปกติและปัญหาที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันท่วงที โดยบันทึกวิเคราะห์และรายงานเหตุการณ์ความปลอดภัยและดำเนินการวิเคราะห์สาเหตุรากฐานของเหตุการณ์ความปลอดภัยเป็นประจำ เพื่อป้องกันไม่ให้เกิดปัญหาดังกล่าวเกิดขึ้นอีก เพื่อสนับสนุนลูกค้าในการตรวจจับและตอบสนองต่อบัณฑิตเหตุอย่างรวดเร็ว Tencent Cloud ให้บริการแพลตฟอร์มการจัดการความปลอดภัยแบบครบวงจร Cloud Security Center (CSC) ผ่านฟังก์ชันต่างๆ เช่น ศูนย์สินทรัพย์ ศูนย์ความเสี่ยง ศูนย์แจ้งเตือน และการจัดการความปลอดภัยขั้นสูง ช่วยลูกค้าบรรลุวงจรการดำเนินงานความปลอดภัยได้แก่ การตรวจจับภัยคุกคามก่อนเกิดเหตุการณ์ตอบสนองและจัดการระหว่างเกิดเหตุการณ์ และการวิเคราะห์ย้อนหลังหลังเหตุการณ์ เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัย	ลูกค้าควรสร้างขั้นตอนการจัดการเหตุการณ์ความปลอดภัยเทคโนโลยีสารสนเทศ เพื่อบันทึก วิเคราะห์ และรายงานเหตุการณ์ความปลอดภัย และดำเนินการวิเคราะห์สาเหตุรากฐานของเหตุการณ์ความปลอดภัยเป็นประจำ เพื่อป้องกันไม่ให้เกิดปัญหาดังกล่าวเกิดขึ้นอีก เพื่อสนับสนุนลูกค้าในการตรวจจับและตอบสนองต่อบัณฑิตเหตุอย่างรวดเร็ว Tencent Cloud ให้บริการแพลตฟอร์มการจัดการความปลอดภัยแบบครบวงจร Cloud Security Center (CSC) ผ่านฟังก์ชันต่างๆ เช่น ศูนย์สินทรัพย์ ศูนย์ความเสี่ยง ศูนย์แจ้งเตือน และการจัดการความปลอดภัยขั้นสูง ช่วยลูกค้าบรรลุวงจรการดำเนินงานความปลอดภัยได้แก่ การตรวจจับภัยคุกคามก่อนเกิดเหตุการณ์ตอบสนองและจัดการระหว่างเกิดเหตุการณ์ และการวิเคราะห์ย้อนหลังหลังเหตุการณ์ เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัย
				ในด้านการจัดการเหตุการณ์ Tencent Cloud ได้กำหนดขั้นตอนการจัดการเหตุการณ์และคำขอรับบริการภายในองค์กร และสร้างกลยุทธ์การจัดการเหตุการณ์ของ Tencent Cloud เพื่อให้มั่นใจว่าเหตุการณ์ที่เกี่ยวข้องกับกิจกรรมการจัดการบริการเทคโนโลยีสารสนเทศได้รับการบันทึกและจำแนกประเภท และจัดลำดับความสำคัญตามผลกระทบและความเร่งด่วน รวมถึงการยกระดับตามความจำเป็น เพื่อแก้ไขและปิดเหตุการณ์ทุกประเภทอย่างรวดเร็ว ทำให้ผลกระทบของเหตุการณ์มีน้อยที่สุด

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโนโลยีสารสนเทศ			รักษาการดำเนินธุรกิจให้เป็นปกติ และเพิ่มความพึงพอใจของลูกค้า ในด้านการสื่อสารและการแจ้งเหตุการณ์ Tencent Cloud ได้กำหนดมาตรฐานการจัดการเหตุการณ์ความปลอดภัย ภัยข้อมูล สร้างขั้นตอนที่เกี่ยวข้อง เช่น การตอบสนองเหตุการณ์ความปลอดภัยข้อมูล การยกระดับเหตุการณ์ และการแจ้งเหตุการณ์ เพื่อแจ้งเตือนหรือแจ้งให้พนักงานภายในบริษัท ลูกค้า และผู้เกี่ยวข้องอื่น ๆ ที่อาจหรือได้รับผลกระทบจากอุบัติเหตุทราบทันเวลา ทำให้ทุกฝ่ายสามารถสื่อสารและประสานงานกันอย่าง เป็นระเบียบ ทันเวลา และมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบ ต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัย ภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียใ ห้เหลือน้อยที่สุด ในด้านการสรุปเหตุการณ์และการปรับปรุงอย่าง ต่อเนื่อง Tencent Cloud ได้สร้างกลไกการวิเคราะห์เหตุการณ์เป็นระยะ โดยจะวิเคราะห์เหตุการณ์หลายมิติเป็นประจำ (ประเภทเหตุการณ์ ความถี่ในการเกิด ขอบเขตผลกระทบ และระดับความรุนแรง) และดำเนินการมาตรการป้องกันตามการทบทวนเหตุการณ์ และการวิเคราะห์สาเหตุรากฐาน เพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่คล้ายคลึงกันเกิดขึ้นอีก สำหรับเหตุการณ์ความปลอดภัยที่สำคัญ Tencent Cloud จะจัดตั้งทีมเฉพาะกิจเพื่อจัดทำรายงานการวิเคราะห์เจ พาะเรื่องเสนอต่อฝ่ายบริหาร ในด้านการที่ลูกค้าแจ้งปัญหาหรือติดต่อ Tencent Cloud

ลำดับที่		โดเมน การคว มคุ้ม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ หารแนว			
2	ความปลอดภัยสารสนเทศ			คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการใช้งาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับ ระบบใช้งานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับทีมงานของลูกค้าผ่านกลไกการตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมและจัดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้าได้รับการตอบสนองและจัดการอย่างทันทางที่ นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้าได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเว ลา ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับกา รสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า
9.1- 9.6	2.9.1-2.9.7	การจัด ทำแผนฉุกเฉิน ด้านเทคโนโลยี สารสนเทศ (IT disaster recovery plan: IT DRP) โดยแผนดังกล่าวต้องไ ด้รับอนุมัติจากคณะกรรมการ ที่ได้รับมอบหมาย	มีคณะทำงานหรือหน วยงานที่รับผิดชอบในก ารจัดทำแผนฉุกเฉินด้าน เทคโนโลยีสารสนเทศ (IT disaster recovery plan: IT DRP) โดยแผนดังกล่าวต้องไ ด้รับอนุมัติจากคณะกรรมการ ที่ได้รับมอบหมาย	ลูกค้าควรสร้างกลไกการจัดการความต่อเนื่องของธุรกิจ ดำเนินการวิเคราะห์ผลกระทบทางธุรกิจ กำหนดเป้าหมายเวลาในการกู้คืน (Recovery Time Objective: RTO) และเป้าหมายจุดข้อมูลในการกู้คืน (Recovery Point Objective: RPO) ของแต่ละธุรกิจให้ชัดเจน จัดทำแผนฉุกเฉินเพื่อความต่อเนื่องของธุรกิจ และสื่อสารไปยังผู้ที่เกี่ยวข้อง นอกจากนี้ ลูกค้ายังควรตรวจสอบและทดสอบการดำเนินการตาม แผนฉุกเฉินอย่างน้อยปีละครั้ง ลูกค้าควรสร้างศูนย์ข้อมูลสำรองเพื่อให้สามารถดำเนิน

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คในโลยีสารสนเทศ		หรือผู้บริหารระดับสูงที่ ได้รับมอบหมายกรณี ปีนสาขานาการพาณิ ชย์ต่างประเทศ จัดทำแผนฉุกเฉินด้าน เทคโนโลยีสารสนเทศ ปีนลายลักษณ์อักษร โดยคำนึงถึง ลักษณะการให้บริการ การดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ ความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศ และความเสี่ยงที่เกี่ยวข้อง แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต้องมี ความเป็นไปได้ในทางป ฏิบัติ สามารถนำมาใช้ รองรับความเสียหายที่เ กิดขึ้นได้จริง และสอดคล้องกับหลักเ กณฑ์อื่นที่เกี่ยวข้องข องธนาคารแห่งประเทศไทย โดยการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรสอดคล้องกับระยะเวลาในการกู้คืนระบบ (recovery time objective : RTO) ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (recovery point object : RPO) และ	การแทนได้เมื่อศูนย์ข้อมูลหลักเกิดการขัดข้อง เพื่อรับประกันความพร้อมใช้งานของธุรกิจ เพื่อให้มั่นใจในความพร้อมใช้งานอย่างต่อเนื่องของธุรกิจลูกค้า Tencent Cloud ได้ออกแบบและนำกรอบการจัดการความต่อเนื่องของธุรกิจที่เหมาะสมกับสภาพแวดล้อมคอมพิวเตอร์คลาวด์ของตนเองไปใช้ และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจ Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภัณฑ์และบริการคลาวด์ กำหนด RTO และ RPO ของแต่ละธุรกิจให้ชัดเจน และจัดทำกลยุทธ์การตอบสนองและแผนความต่อเนื่องของธุรกิจที่แตกต่างกันตามผลการวิเคราะห์ผลกระทบทางธุรกิจ รวมถึงจัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดยละเอียดสำหรับผลิตภัณฑ์คลาวด์ ในด้านการสนับสนุนบุคลากร Tencent Cloud ได้กำหนดบทบาทของบุคลากรในกระบวนการกู้คืนธุรกิจ และกำหนดหน้าที่และความรับผิดชอบในการแบ่งงานกันในกระบวนการกู้คืนให้ชัดเจน สำหรับทักษะหรือตำแหน่งงานที่สำคัญ ใช้กลไกเสริม A/B Role และดำเนินการฝึกอบรมซ้อมแผนฉุกเฉินเป็นประจำเพื่อรับประกันการดำเนินการขั้นตอนการกู้คืนที่รวดเร็วและมีประสิทธิภาพ ร่วมกับลูกค้าในการบรรลุการกู้คืนทันเวลาที่ในสถานการณ์ที่ธุรกิจขัดข้อง ในด้านการฝึกซ้อมความต่อเนื่องของธุรกิจและการกู้คืนจากภัยพิบัติ Tencent Cloud จัดทำแผนการฝึกซ้อมโดยอิงตามแผนความต่อเนื่องของธุรกิจ และดำเนินการประเมินความเสี่ยงในการฝึกซ้อมพร้อมกำหนดมาตรการรับประกันที่สอดคล้องกันเพื่อหลีกเลี่ยงผลกระทบเชิงลบต่อบริการจากการฝึกซ้อม การฝึกซ้อมการกู้คืนจากภัยพิบัติของ Tencent Cloud มักดำเนินการโดยจำลองสถานการณ์การกู้คืนจากภัย

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร รแบบ	แนวปฏิบัติในการบริ หารความเสี่ยงด้านเท คโนโลยีสารสนเทศ			
2	คโนโลยีสารสนเทศ		ระยะเวลาสูงสุดที่ยอมให้ ให้การให้บริการหรือธุรกิจหยุดชะงัก (maximum tolerance period of disruption : MTPD) เพื่อรองรับการให้บริการหรือดำเนินธุรกิจอย่างต่อเนื่องของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ มีคู่มือหรือเอกสารประกอบการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ รวมทั้งประชาสัมพันธ์และฝึกอบรมเพื่อให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการดำเนินการตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศมีความเข้าใจและสามารถปฏิบัติตามแผนดังกล่าวได้ ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อย ปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ มีศูนย์คอมพิวเตอร์สำรอง (disaster recovery site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อ	ปฏิบัติตามคลาสิกที่สมจริง รวมถึงการต่อสู้ป้องกันการโจมตีและความล้มเหลวขนาดใหญ่ เพื่อตรวจสอบความสามารถในการกู้คืนจากภัยพิบัติของระบบ ความเร็วในการตอบสนอง และความสามารถในการกู้คืนอย่างครอบคลุม สำหรับปัญหาที่ค้นพบระหว่างการฝึกซ้อม Tencent Cloud จะดำเนินการแก้ไขตามมาตรการปรับปรุงที่ระบุไว้ในรายงานสรุปการฝึกซ้อม และแก้ไขแผนฉุกเฉินที่เกี่ยวข้องทันที โดยฝ่ายตรวจสอบจะกำกับดูแลและตรวจสอบสถานการณ์การแก้ไข เพื่อช่วยลูกค้าสร้างศูนย์ข้อมูลสำรอง ศูนย์ข้อมูลของ Tencent Cloud มีอยู่ทั่วโลกหลายภูมิภาคทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) ครอบคลุมพื้นที่จีนแผ่นดินใหญ่ ภูมิภาคเอเชียแปซิฟิก ภูมิภาคอเมริกาเหนือ และภูมิภาคยุโรป ลูกค้าสามารถปรับใช้ข้อมูลและระบบในภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระและยืดหยุ่นตามความต้องการในการพัฒนาธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติ (disaster recovery) ของธุรกิจ จุดทางออกเครือข่ายของแต่ละโซนความพร้อมใช้งานเชื่อมต่อกับผู้ให้บริการหลายราย เพื่อสร้างความสามารถในการกู้คืนจากภัยพิบัติข้ามภูมิภาคของเครือข่าย Tencent Cloud และลดผลกระทบที่ต่อเนื่องจากการขัดข้องของเครือข่ายสถานะของผู้ให้บริการอย่างมีประสิทธิภาพ เครือข่ายพื้นฐานของ Tencent Cloud ใช้วิธีการก่อสร้างแบบซ้ำซ้อน ร่วมกับการจัดลำดับความสำคัญของเส้นทางในระดับการกำหนดเส้นทางและการจัดสรรการจราจรเพื่อความสามารถในการเข้าถึงเส้นทาง เพื่อให้มั่นใจว่าบริการเครือข่ายจะไม่หยุดชะงักเนื่องจากความล้มเหลวของอุปกรณ์จุดเดียว

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร	แนวปฏิบัติในการบริ			
รแบบ	หาความเสี่ยงด้านเท			
2	คโณโลยีสารสนเทศ		ศูนย์คอมพิวเตอร์หลัก (primary site) ภัยชะงัก โดยศูนย์คอมพิวเตอร์สำรอง ควรอยู่ห่างจากศูนย์คอมพิวเตอร์หลักเพียงพอที่จะมิให้เกิดปัญหาหรือได้รับผลกระทบในลักษณะเดียวกัน ในช่วงเวลาเดียวกัน เช่น ระบบไฟฟ้าขัดข้อง และภัยธรรมชาติเป็นต้น	โหนดการคำนวณของ Tencent Cloud ยังใช้วิธีการก่อสร้างแบบซ้ำซ้อน โดยเมื่อโหนดการคำนวณเดียวเกิดความล้มเหลวจะถูกตัดออกโดยอัตโนมัติแบบเรียลไทม์ผ่านตัวจัดการกำหนดการ ซึ่งรับประกันความพร้อมใช้งานของธุรกิจลูกค้าได้อย่างมีประสิทธิภาพ
10.1 、 10.5	2.10.1	การบริหารจัดการความเสี่ยงจากบุคคลภายนอก	ในกรณีที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจดำเนินการดังต่อไปนี้ (1) ใช้บริการงานด้านเทคโนโลยีสารสนเทศจากบุคคลภายนอก (IT outsourcing) (2) เชื่อมต่อระบบเทคโนโลยีสารสนเทศกับบุคคลภายนอก หรือ (3) ให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือเข้าถึงข้อมูลลูกค้าในรูปแบบอิเล็กทรอนิกส์สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องกำกับดูแลความเสี่ยงการรักษาความมั่นคงป	หากลูกค้ามอบบริการเทคโนโลยีสารสนเทศให้บุคคลที่สามดำเนินการแทน หรือเชื่อมโยงระบบเทคโนโลยีสารสนเทศกับบุคคลที่สามหรืออนุญาตให้บุคคลที่สามเข้าถึงข้อมูลสำคัญทางอิเล็กทรอนิกส์ ควรควบคุมดูแลความปลอดภัยเครือข่ายและเทคโนโลยีสารสนเทศของบุคคลที่สามตามระดับความเสี่ยงและความสำคัญ เพื่อให้มั่นใจในความรับผิดชอบในการให้บริการความต่อเนื่องทางธุรกิจ และคุณภาพ ฯลฯ Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสองฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์

เอกสารแนบ	ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
2	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ		ลดภัยด้านเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยจากภัยไซเบอร์ให้สอดคล้องตามระดับความเสี่ยงและระดับความมั่นคงสำคัญบนพื้นฐานที่ต้องรับผิดชอบต่อการให้บริการหรือดำเนินธุรกิจแก่ลูกค้าและคงไว้ซึ่งความน่าเชื่อถือ ชื่อเสียงประสิทธิภาพในการให้บริการ	เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้บริการคลาวด์ที่ Tencent Cloud มอบให้แก่ลูกค้ามีการส่งมอบตามข้อตกลงระดับการให้บริการ (SLA) ที่ตกลงกันสำหรับแต่ละบริการตัวชี้วัดประสิทธิภาพ เกณฑ์การวัดและข้อกำหนดในการรายงานสำหรับบริการแต่ละรายการกำหนดไว้อย่างชัดเจนใน SLA ของผลิตภัณฑ์แต่ละรายการและเผยแพร่บนเว็บไซต์อย่างเป็นทางการของ Tencent Cloud Tencent Cloud จะติดตามประสิทธิภาพและความพร้อมใช้งานของบริการคลาวด์อย่างต่อเนื่องและให้การตรวจสอบแบบเรียลไทม์แก่ลูกค้าผ่านคอนโซลการจัดการ เนื้อหาของข้อกำหนดนี้สอดคล้องกับภาคผนวก "แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก" เป็นอย่างยิ่งสำหรับเนื้อหารายละเอียดเพิ่มเติมเกี่ยวกับการจัดการความเสี่ยงของบุคคลที่สาม โปรดดูที่ "5.7 แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก" ในคู่มือนี้

5.4 เอกสารแนบ 3

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

เอกสารแนบ	ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
2	1.2.7	การปฏิบัติงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	การปฏิบัติงานด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศกำหนดให้มีระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ (IT risk appetite)	ลูกค้าควรกำหนดกรอบการจัดการความเสี่ยงดำเนินการปฏิบัติการจัดการความเสี่ยงและมาตรการควบคุมที่มีประสิทธิภาพและกำหนดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud

ลำดับที่		โดเมนการควบคุม	ข้อกำหนดความคุ้มครองเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
3	นโยบายสารสนเทศ	ทศ	โดยได้รับการอนุมัติจากคณะกรรมการที่ได้รับมอบหมายหรือผู้บริหารระดับสูงที่ได้รับมอบหมายกรณีเป็น สาขาธนาคารพาณิชย์ต่างประเทศรวมทั้งมีการจัดทำกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยประสานงานร่วมกับหน่วยงานที่ทำหน้าที่เป็น first line of defence ในการระบุและประเมินความเสี่ยงการกำหนดมาตรการลดความเสี่ยงและระบบการควบคุมภายใน	ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามงานต่างๆ เช่น การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยงไว้อย่างชัดเจน Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุความเสี่ยงตามสถานการณ์ความเสี่ยงผลิตภัณฑ์ทางธุรกิจ หรือกระบวนการให้บริการสำหรับความเสี่ยงที่ระบุได้ Tencent Cloud จะประเมินความเป็นไปได้และระดับผลกระทบของความเสี่ยงแต่ละรายการเพื่อจำแนกระดับความเสี่ยงและดำเนินการตามขั้นตอนที่สอดคล้องกันต่อไป โดยมีกระบวนการทบทวนการประเมินความเสี่ยงทั้งหมดไว้ Tencent Cloud ยังติดตามสถานการณ์การจัดการความเสี่ยงอย่างต่อเนื่อง ประเมินความเสี่ยงที่เหลืออยู่ และให้มั่นใจว่าผู้เกี่ยวข้องได้จัดการความเสี่ยงอย่างเหมาะสมตามข้อกำหนดการจัดการความเสี่ยงของ Tencent Cloud นอกจากนี้ Tencent Cloud บำรุงรักษาและปรับปรุงวิธีการประเมินความเสี่ยงและทะเบียนความเสี่ยงอย่างต่อเนื่องตามแนวโน้มการเปลี่ยนแปลงในอุตสาหกรรมตลาดและแนวปฏิบัติการจัดการภายใน
2.1	1.2.7	การประเมินความเสี่ยง	การระบุความเสี่ยงให้ระบุถึงความเสี่ยงด้านเทคโนโลยีสารสนเทศซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงานระบบงาน บุคลากร การใช้บริการจากบุคคลภายนอก หรือปัจจัยภายนอก การวิเคราะห์ความเสี่ยง	ลูกค้าควรระบุภัยคุกคามและช่องโหว่ที่ใช้ได้กับสภาพแวดล้อมเทคโนโลยีสารสนเทศของตนเองเป็นประจำ วิเคราะห์และประเมินความเสี่ยงที่เกิดจากภัยคุกคามและช่องโหว่เหล่านี้ จัดลำดับความสำคัญของความเสี่ยง จัดทำมาตรการลดความเสี่ยง ประเมินความเสี่ยงที่เหลืออยู่ และติดตามประสิทธิภาพของมาตรการควบคุมความเสี่ยง Tencent Cloud ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามและให้คำแนะนำเกี่ยวกับเนื้อหาการทำงานของกระบวนการจัดการความเสี่ยงทั้งหมด (การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยง)

ลำดับที่		โดเมน	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	การควบคุม		
3	นโยบายสารสนเทศ		ง ควรเข้าใจและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม การประเมินค่าความเสี่ยง ให้ประเมินถึงโอกาสที่ความเสี่ยงด้านเทคโนโลยีสารสนเทศจะเกิดขึ้นและส่งผลกระทบต่อการปฏิบัติงาน	ไว้อย่างชัดเจน • การระบุความเสี่ยง: Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุสถานการณ์ความเสี่ยงที่ใช้ได้กับ Tencent Cloud จากแหล่งต่างๆ เช่น รายงานเหตุการณ์ความปลอดภัยในอุตสาหกรรม การสะสมประสบการณ์การปฏิบัติของ Tencent Cloud • การประเมินความเสี่ยง: Tencent Cloud ประเมินมูลค่าสินทรัพย์ ความเป็นไปได้ของความเสี่ยงในสถานการณ์ความเสี่ยง และระดับผลกระทบของความเสี่ยง และคำนวณระดับความเสี่ยง • การจัดการความเสี่ยง: ตามผลการวิเคราะห์ความเสี่ยง สำหรับความเสี่ยงที่ระบุ Tencent Cloud จะใช้กลยุทธ์การตอบสนองและมาตรการบรรเทา ความเสี่ยงที่สอดคล้องกัน สำหรับความเสี่ยงสูง ผู้รับผิดชอบด้านความเสี่ยงจะจัดทำแผนจัดการ ความเสี่ยง (มาตรการการโอนย้ายหรือลดความเสี่ยง) และอัปเดตตารางการจัดการความเสี่ยง สำหรับความเสี่ยงปานกลาง ผู้รับผิดชอบด้านความเสี่ยงจะตัดสินใจตามสภาพแวดล้อมจริงว่าจำเป็นต้องจัดทำแผนจัดการ ความเสี่ยงหรือไม่ สำหรับความเสี่ยงต่ำถือเป็นความเสี่ยงที่ยอมรับได้ สำหรับความเสี่ยงที่เหลือ Tencent Cloud จะทบทวนทุกครั้ง เพื่อตรวจสอบสถานะและมูลค่าความเสี่ยง • การติดตาม การทบทวน และการรายงานความเสี่ยง: Tencent Cloud รวมผลการประเมินความเสี่ยง ออกรายงานการประเมินความเสี่ยง
2.2	1.2.7	การจัดก ารความ เสี่ยง	การจัดการความเสี่ยง ต้องมีแนวทางจัดการ ความควบคุม และป้องกันความเสี่ยง ที่เหมาะสม สอดคล้องกับผลการ ประเมินความเสี่ยงด้าน เทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลือ อยู่ (residual risk) อยู่ในระดับความเสี่ยง ด้านเทคโนโลยีสารสนเทศ ที่ยอมรับได้ (IT risk appetite) ทั้งนี้ ต้องกำหนดดัชนีชี้วัด ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำคัญ (IT key risk indicators) ที่เกี่ยวข้องกับการให้ บริการหรือดำเนินธุรกิจ ให้สอดคล้องกับความ สำคัญของเทคโนโลยีสารสนเทศ แต่ละงาน	

ลำดับที่		โดเมน การคว บคุม	ข้อกำหนดความค มเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร รแบบ	แนวปฏิบัติในการบริหาร ความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
3	นโยบายสารสนเทศ		เพื่อใช้ติดตามและทบท วนความเสี่ยง	และรายงานต่อฝ่ายบริหาร และบำรุงรักษาตารางการจัดการความเสี่ยง ติดตามการเปลี่ยนแปลงเงื่อนไขความเสี่ยงและส ถานะของแผนจัดการความเสี่ยง และปรับแผนการจัดการความเสี่ยงแบบเรียลไทม์
2.3	1.2.7	ตรวจสอบความเสี ยด้วยกา รตรวจสอบ	การติดตามและทบท วนความเสี่ยง ต้องมีกระบวนการที่มีป รสิทธิภาพในการติดต าม และทบทวนความเสี่ยง ด้านเทคโนโลยีสารสนเทศ เพื่อให้อยู่ภายใต้ระดับค วามเสี่ยงด้านเทคโนโลยี สารสนเทศ ที่ยอมรับได้ที่กำหนดไว้	นอกจากนี้ Tencent Cloud ยังกำหนดตัวชี้วัดความเสี่ยงที่สำคัญและวัดตัวชี้วัดคว ามเสี่ยงที่สำคัญเป็นประจำ เทียบเคียงกับเกณฑ์ความเสี่ยงที่ยอมรับได้ วิเคราะห์สาเหตุรากฐานของปัญหาที่พบ และเสนอข้อเสนอนะและแนวทางในการปรับปรุง
2.4	1.2.7	รายงานค วามเสี่ยง	การรายงานความเสี่ยง ให้รายงานระดับความ เสี่ยงและผลการบริหาร ความเสี่ยงด้าน เทคโนโลยีสารสนเทศ ต่อคณะกรรมการของ สถาบันการเงินหรือค ณะกรรมการของสถา บันการเงินเฉพาะกิจ หรือคณะกรรมการที่ไ ด้รับมอบหมาย หรือผู้บริหารระดับสูงที่ ได้รับมอบหมายกรณี เป็นสาขานาการพาณิชย์ ต่างประเทศเป็นประจำ อย่างสม่ำเสมอ	

5.5 เอกสารแนบ 4

การกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ
ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

ลำดับที่		โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
4	นโยบายสารสนเทศ		กำหนดกระบวนการในการกำกับดูแลการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยอย่างน้อยครอบคลุม ดังนี้:	ลูกค้าควรกำหนดขั้นตอนและระบบสำหรับการปฏิบัติตามกฎระเบียบที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ระบุกฎหมายที่ต้องปฏิบัติตาม จัดทำแผนการจัดการความเสี่ยงด้านการปฏิบัติตามข้อกำหนดประจำปี และดำเนินการตรวจสอบการปฏิบัติตามข้อกำหนดเป็นประจำ ติดตามและรายงานผล
2.1-2.3	1.2.8	การปฏิบัติงานด้านการกำกับดูแลการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	การระบุและประเมินความเสี่ยงด้านการปฏิบัติตามกฎหมาย ต้องครอบคลุมถึงกฎหมายและกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	ในด้านการปฏิบัติตามข้อกำหนด, Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด และได้สร้างขั้นตอนที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านความปลอดภัย เพื่อให้มั่นใจว่าการดำเนินการด้านความปลอดภัยข้อมูลเป็นไปตามข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ มาตรฐาน และขั้นตอนที่เกี่ยวข้อง ทีมงานฝ่ายกฎหมายของ Tencent Cloud จะระบุและรวบรวมข้อกำหนดการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับธุรกิจของ Tencent Cloud อย่างต่อเนื่อง จัดทำเป็นรายการกฎหมายและระเบียบข้อบังคับที่สอดคล้องกัน และบำรุงรักษาและปรับปรุงเป็นประจำ
			การกำหนดแผนการบริหารความเสี่ยงด้านการปฏิบัติงานตามกฎหมาย (compliance program) ประจำปี ต้องครอบคลุมถึงกฎหมายและกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	
			การติดตามและรายงานผลการสอบทานด้านการปฏิบัติตามกฎหมาย สรุปผลเหตุการณ์ ไม่ปฏิบัติตามกฎหมายและมาตรการแก้ไข รวมถึงผลการดำเนินการตามข้อเสนอแนะคำสั่งของ อปท. และผู้กำกับดูแลอื่นที่เกี่ยวข้อง ต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย	ในด้านการตรวจสอบและการทบทวน, Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์ และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็นอิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้กับการสำรวจของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ 4	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	กรณีเป็นสาขานาคารพาณิชย์ต่างประเทศเป็นประจำอย่างสม่ำเสมอ	หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง ศูนย์ความปลอดภัยแพลตฟอร์มคลาวด์จะประเมินและยืนยันการปฏิบัติตามนโยบายและขั้นตอนความปลอดภัยเป็นประจำ โดยขอบเขตการประเมินรวมถึงการรั่วไหลของข้อมูลที่ละเอียดอ่อน การลดช่องโหว่ด้านความปลอดภัย การกำหนดค่าความปลอดภัย เป็นต้น

5.6 เอกสารแนบ 5

การตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ 5	แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	กำหนดขอบเขตการตรวจสอบต้องครอบคลุมการปฏิบัติงาน กระบวนการทำงานและระบบงานด้านเทคโนโลยีสารสนเทศทั้งหมด รวมทั้งการใช้บริการ การเชื่อมต่อหรือการเข้าถึงจากบุคคลภายนอก เพื่อให้สามารถระบุและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างครบถ้วน โดยมีกระบวนการอย่างน้อยครอบคลุมดังนี้	ลูกค้าควรกำหนดแผนการตรวจสอบเทคโนโลยีสารสนเทศที่สอดคล้องกับความสำเร็จและระดับความเสี่ยงของการใช้เทคโนโลยีสารสนเทศ ดำเนินการตรวจสอบตามแผนและขอบเขตการตรวจสอบอย่างน้อยปีละหนึ่งครั้ง ดำเนินการตรวจสอบเมื่อเกิดกิจกรรมด้านเทคโนโลยีสารสนเทศที่สำคัญหรือเมื่อเกิดเหตุการณ์ความผิดปกติด้านเทคโนโลยีสารสนเทศที่สำคัญ รายงานผลการตรวจสอบ และติดตามการแก้ไขปัญหาที่พบจากการตรวจสอบ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud
2.1-2.3	1.2.9 การปฏิบัติงานการตรวจสอบเทคโนโลยีสารสนเทศ	การกำหนดแผนงานตรวจสอบ ต้องสอดคล้องกับความสำเร็จและความเสี่ยงของ	จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเทศไทย ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัย

เอกสารแนบ	ลำดับที่ แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
5	นโยบายสารสนเทศ		การใช้งานเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ สำหรับงานด้านเทคโนโลยีสารสนเทศที่มีนัยสำคัญ ต้องตรวจสอบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งเมื่อมีเหตุการณ์ผิดปกติในเทคโนโลยีสารสนเทศที่มีนัยสำคัญ การตรวจสอบ ต้องตรวจสอบตามแผนงานและขอบเขตที่กำหนดอย่างน้อย ปีละ 1 ครั้ง การติดตามและรายงานผลการตรวจสอบ ต้องสรุปผลการตรวจสอบและประเด็นที่ต้องแก้ไขกับผู้บริหารของหน่วยงานผู้รับตรวจและจัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอต่อคณะกรรมการตรวจสอบและแจ้งให้ผู้บริหารระดับสูงที่เกี่ยวข้องรับทราบ รวมถึงติดตามให้มีการปรับปรุง ประเด็นการตรวจสอบและรายงานประเด็นสำคัญพร้อมแผนปรับปรุงให้กับคณะกรรมการตรวจสอบ เป็นประจำอย่างสม่ำเสมอ ทั้งนี้ ให้จัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่สถาบันการเงินและสถาบันก	ภัยภายในอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบการจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็นอิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้กับการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว สำหรับข้อที่ไม่สอดคล้องที่พบจากการตรวจสอบ Tencent Cloud จะวิเคราะห์สาเหตุจริงหรือสาเหตุที่มีศักยภาพที่ทำให้เกิดข้อที่ไม่สอดคล้องอย่างทันที่ ประเมินความต้องการและลำดับความสำคัญของการดำเนินการมาตรการแก้ไขและป้องกัน และดำเนินการมาตรการแก้ไขและป้องกันหลังจากได้รับอนุมัติที่เกี่ยวข้อง ประสิทธิภาพของการดำเนินการมาตรการแก้ไขจะถูกติดตามและบันทึกอย่างต่อเนื่อง

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบปฏิบัติการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
5	นโยบายสารสนเทศ	การเงิน เฉพาะกิจ เพื่อให้พร้อมสำหรับการ ตรวจสอบหรือเมื่อร้องขอ โดย ธปท.	

5.7 แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

5.7.1 การกำกับดูแลการบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
6	การตรวจสอบ	6.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกที่ได้รับภารแต่งตั้งจากสถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถเข้าตรวจสอบบุคคลภายนอกในส่วนที่เกี่ยวข้องกับการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจได้ เช่น ระบุเงื่อนไขในสัญญาหรือ ข้อตกลง เป็นต้น สำหรับผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก มีสิทธิเข้าตรวจสอบการดำเนินการด้านเทคโนโลยีสารสนเทศของบุคคลภายนอก ในเงื่อนไขสัญญา หรือข้อตกลงได้สถาบันการเงินและสถาบันการเงินเฉพาะกิจต้องมั่นใจว่าบุคคลภายนอกรายดังกล่าวมีผลการตรวจสอบจากผู้ตรวจสอบภายนอกที่เป็นอิสระทดแทนได้ 6.2 จัดให้มีการตรวจสอบให้สอดคล้องตามขอบเขต	ลูกค้าควรทำให้มั่นใจว่าธนาคารแห่งประเทศไทย หน่วยงานตรวจสอบภายใน หรือสถาบันตรวจสอบบุคคลที่สามารถดำเนินการตรวจสอบบริการภายนอกที่ใช้อยู่ หรือผู้ให้บริการจัดทำรายงานตรวจสอบที่เทียบเท่าเป็นหลักฐาน ลูกค้าควรดำเนินการตรวจสอบบุคคลที่สามที่สำคัญอย่างน้อยปีละหนึ่งครั้ง ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบการจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็นอิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ระดับความเสี่ยงและความมีนัยสำคัญ จากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่มีนัยสำคัญควรได้รับการตรวจ สอบอย่าง น้อยปีละ 1 ครั้ง และเมื่อพบเหตุการณ์ผิดปกติที่มีนัย สำคัญ ทั้งนี้ หากมีเหตุจำเป็นที่สถาบันการเงินแ ละสถาบันการเงินเฉพาะกิจไม่สามารถ ดำเนินการตรวจสอบได้ สถาบันการเงินและสถาบันการเงินแ เฉพาะกิจควรมีแนวทางที่จะใช้ประเมิน หรือติดตามการดำเนินงาน และการควบคุมภายในของบุคคลภา ยนอกให้รัดกุมเพียงพอสอดคล้องตาม ขอบเขต ระดับความ เสี่ยง และความมีนัยสำคัญของการใช้บริ การ การเชื่อมต่อหรือการเข้าถึงข้อมูล โดยอาจใช้ผลการ ตรวจสอบด้านเทคโนโลยีสารสนเทศ ของบุคคลภายนอกที่ได้รับการรับ รองจากผู้ตรวจสอบภายนอกที่ มีความเป็นอิสระและได้มาตรฐานสา เป็นต้น และรับทราบโดย คณะกรรมการหรือผู้บริหารระดับสูง ที่ได้รับมอบหมายแล้วได้	ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่ สามที่เป็นอิสระแล้ว Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์ จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเท ศไทย

5.7.2 การบริหารจัดการความเสี่ยงจากบุคคลภายนอก

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
8	การคัดเลือกบุ คคลภายนอก	8.1 สถาบันการเงินและสถาบันการเงิน เฉพาะกิจควรกำหนดให้มีระเบียบวิ ธีปฏิบัติและหลักเกณฑ์ใน การพิจารณาคัดเลือกบุคคลภายนอก อย่างชัดเจน และเป็นลายลักษณ์อักษร โดยมีข้อมูลที่เพียงพอ สำหรับสนับสนุนการพิจารณาตัดสิน ใจใช้บริการเชื่อมต่อหรือการเข้าถึง ข้อมูลจากบุคคลภายนอก เพื่อ	ลูกค้าควรกำหนดขั้นตอนและมาตรฐานการประเมินและ เลือกบริการบุคคลที่สามอย่างชัดเจน และการตัดสินใจร่วมมือกับบุคคลที่สามที่มีความเสี่ยงสูงห ือผลกระทบอย่างมีนัยสำคัญควรได้รับการอนุมัติจากฝ่ ายบริหาร นอกจากนี้ ลูกค้าควรดำเนินการตรวจสอบอย่างละเอียดต่อบุคคลที่ส ามตามเกณฑ์การประเมิน โดยมุ่งเน้นการประเมินชื่อเสียงทางธุรกิจ ความแข็งแกร่งทางการเงินและทรัพยากร กรอบและความสามารถในการจัดการความเสี่ยง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		สามารถคัดเลือกบุคคลภายนอกที่มีความเหมาะสมตามวัตถุประสงค์การดำเนินการของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ	มาตรการควบคุมความปลอดภัยทางเทคโนโลยีสารสนเทศ การจัดเตรียมการกู้คืนจากภัยพิบัติ ความสามารถในการปฏิบัติตามและบันทึกการปฏิบัติตามข้อกำหนดของผู้ให้บริการบุคคลที่สาม
	8.2 การตัดสินใจใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่มีความเสี่ยงหรือมี	นัยสำคัญควรได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย	Tencent Cloud ได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบอย่างละเอียดของลูกค้าอย่างเข้มข้น ต่อไปนี้เป็นภาพรวมของ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ในด้านต่างๆ ของการตรวจสอบอย่างละเอียด:
	8.3 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรทำการประเมินศักยภาพบุคคลภายนอก (due diligence) โดยพิจารณาประเมินให้ครอบคลุมตามขอบเขต	ระดับความเสี่ยงและความมีนัยสำคัญ โดยควรคำนึงถึงเรื่องดังต่อไปนี้	สภาพทางการเงิน: Tencent Cloud ซึ่งเป็นแบรนด์คอมพิวเตอร์คลาวด์ที่ Tencent Group สร้างขึ้นด้วยความอุสาหะ ได้รับประโยชน์จากความแข็งแกร่งทางการเงินและสภาพทางการเงินที่มั่นคงของ Tencent Group นับตั้งแต่ปี 2010 ที่ Tencent Cloud เริ่มให้บริการคลาวด์แก่สาธารณะอย่างเป็นทางการ Tencent Cloud ได้บรรลุแนวโน้มการเติบโตที่โดดเด่นในตัวชี้วัดทางการเงินที่สำคัญ เช่น รายได้และผลกำไร Tencent Cloud ได้รับการยอมรับจากสถาบันวิจัยอุตสาหกรรมระดับโลกชั้นนำ Gartner ติดต่อกันเป็นเวลาสี่ปี โดยอยู่ในอันดับที่สองในด้านมิติด้านกลยุทธ์ในหมวดผู้ผลิตจากประเทศจีน
	(1) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์และความสามารถในการให้บริการของบุคคลภายนอกในช่วงที่ผ่านมา		
	(2) ธรรมาภิบาลและวัฒนธรรมองค์กรของบุคคลภายนอก		ชื่อเสียงทางธุรกิจ: ในฐานะแบรนด์คอมพิวเตอร์คลาวด์ภายใต้การนำของ Tencent ซึ่งเป็นบริษัทชั้นนำในอุตสาหกรรมอินเทอร์เน็ตของจีน Tencent Cloud ได้รับการรับรองจากสถาบันอุตสาหกรรมหลายแห่ง มอบโซลูชันคอมพิวเตอร์คลาวด์ที่ครอบคลุม และได้ร่วมมือกับพันธมิตรมากกว่า 11,000 ราย เพื่อมอบโซลูชันอุตสาหกรรมมากกว่า 400 รายการให้กับลูกค้าธุรกิจในกว่า 30 อุตสาหกรรม
	(3) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผล การปฏิบัติงาน		ความสามารถทางวิชาชีพและทางเทคนิค: Tencent Cloud ได้แสดงความสามารถทางเทคนิคที่ครอบคลุมในฐานะผู้นำในอุตสาหกรรมผ่านเทคโนโลยีคอมพิวเตอร์คลาวด์ที่แข็งแกร่ง ความสามารถในการประมวลผลข้อมูลขนาดใหญ่
	(4) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ		
	(5) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ		
	(6) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง		
	(7) การปฏิบัติตามมาตรฐานสากล		

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		เทคโนโลยีสารสนเทศ (8)ปัจจัยภายนอกที่อาจกระทบต่อการให้บริการของบุคคลภายนอก (9)การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลง เทคโนโลยีผู้ให้บริการหรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมา ดำเนินการเอง	การประยุกต์ใช้ปัญญาประดิษฐ์ การป้องกันความปลอดภัยทางไซเบอร์ เทคโนโลยีคลาวด์เนทีฟ การกระจายตัวของศูนย์ข้อมูลทั่วโลก และโซลูชันอุตสาหกรรม ความสามารถทางเทคนิคเหล่านี้ไม่เพียงรับประกันความมั่นคงและความน่าเชื่อถือของบริการ Tencent Cloud เท่านั้น แต่ยังจัดเตรียมสภาพแวดล้อมคอมพิวเตอร์คลาวด์ที่ปลอดภัยและน่าเชื่อถือให้กับลูกค้าด้วย ความสามารถด้านความปลอดภัยในการดำเนินงานที่ครบถ้วนของ Tencent Cloud ยังสามารถให้การสนับสนุนทางเทคนิครอบนาฬิกาสำหรับผลิตภัณฑ์คลาวด์แก่ลูกค้าได้ • ประสบการณ์ที่ผ่านมาและความสามารถในการให้บริการ: Tencent Cloud สามารถปรับโซลูชันให้เหมาะสมตามความต้องการของลูกค้า ปรับตัวได้อย่างยืดหยุ่นกับวัฒนธรรมและกลยุทธ์ขององค์กรที่แตกต่างกัน Tencent Cloud ได้ปรับแต่งโซลูชันต่างๆ ให้เหมาะสมสำหรับสถาบันการเงินหลายแห่ง มอบบริการคลาวด์เฉพาะสำหรับการเงินที่สอดคล้องกับข้อกำหนดด้านกฎระเบียบให้กับลูกค้าทางการเงินหลายราย และมีขีดความสามารถในการปฏิบัติตามข้อกำหนดด้านความปลอดภัยระดับการเงิน • โครงสร้างการกำกับดูแลและวัฒนธรรมองค์กร: Tencent Cloud มีเป้าหมาย "เสริมสร้างภูมิคุ้มกันปลอดภัยดิจิทัลขององค์กร สนับสนุนการพัฒนาที่มีความยืดหยุ่นในยุคดิจิทัล" มุ่งมั่นปรับปรุงระบบความปลอดภัยบนคลาวด์ของตนเอง สร้างขีดความสามารถด้านความปลอดภัยและการปฏิบัติตามข้อกำหนด และกำหนดมาตรฐานความปลอดภัยบนคลาวด์ Tencent Cloud ได้จัดตั้งคณะกรรมการเทคโนโลยีความปลอดภัยและทีมงานความปลอดภัยมืออาชีพที่มีหน้าที่และสาขาวิชาที่แตก

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ต่างกัน Tencent Cloud รวบรวมทีมบริการผู้เชี่ยวชาญที่มีประสบการณ์ในอุตสาหกรรม มุ่งมั่นให้บริการผลิตภัณฑ์และบริการที่ปลอดภัย น่าเชื่อถือ เป็นมืออาชีพ และเป็นไปตามข้อกำหนดแก่ลูกค้า การจัดการความเสี่ยง: Tencent Cloud ได้กำหนดกรอบการกำกับดูแลความเสี่ยงและขั้นตอนที่เกี่ยวข้อง และปรับปรุงมาตรการจัดการความเสี่ยงและระบบตรวจสอบภายในอย่างต่อเนื่อง โดยการเสริมสร้างวัฒนธรรมความเสี่ยงอย่างต่อเนื่อง Tencent Cloud ปรับปรุงความสามารถในการจัดการความเสี่ยงภายในอย่างมีประสิทธิภาพ และรับประกันการพัฒนาทางธุรกิจที่ยั่งยืนและมีสุขภาพดี การควบคุมภายในและการตรวจสอบภายใน: Tencent Cloud ดำเนินการทดสอบความปลอดภัย การประเมินความเสี่ยง และการตรวจสอบภายในอย่างเป็นประจำสำหรับระบบสารสนเทศ เพื่อให้แน่ใจว่าการป้องกันความปลอดภัยอยู่ในสถานะที่สมเหตุสมผลอยู่เสมอ และเป็นไปตามข้อกำหนดและข้อกำหนดของการจัดการความปลอดภัยและมาตรฐานที่เกี่ยวข้อง ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละครั้ง และติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้แน่ใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามกฎหมาย ระเบียบข้อบังคับ และมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง การรับประกันความปลอดภัยเทคโนโลยีสารสนเทศ: ใช้สถาปัตยกรรมความปลอดภัยเครือข่ายที่ออกแบบตามแนวปฏิบัติในอุตสาหกรรมเป็นข้อมูลอ้างอิง โดยแบ่งเขตความปลอดภัยตามฟังก์ชันทางธุรกิจและความเสี่ยงด้านความปลอดภัย และแยกพื้นที่ความปลอดภัยต่างๆ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ทางกายภาพหรือทางตรรกะ และใช้มาตรการต่างๆ เช่น การควบคุมการเข้าถึงและการป้องกันขอบเขต เพื่อรับประกันความปลอดภัยของเครือข่ายสำนักงาน เครือข่ายการพัฒนา เครือข่ายทดสอบ และเครือข่ายการผลิต Tencent Cloud ใช้กลไกป้องกันหลายชั้น เช่น ไฟร์วอลล์ ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) การป้องกัน DDoS และการป้องกันความปลอดภัยเว็บ เพื่อตรวจจับ กรอง และป้องกันการรับส่งข้อมูลเครือข่ายที่เป็นอันตรายได้อย่าง ทันท่วงที ปกป้องความปลอดภัยของเครือข่าย Tencent Cloud Tencent Cloud มีกลไกความปลอดภัย เช่น นโยบายการควบคุมการเข้าถึงทรัพยากรในชั้นควบคุมเส มือน (Virtualization Control Layer) นโยบายการแยกระหว่างเครือข่ายส่วนตัวภายในแพลตฟอร์ม ฟอร์มคลาวด์ การจัดสรรสิทธิ์และการยืนยันตัวตนบนเว็บคอนโซล รหัสเซสชันของอินเทอร์เน็ตเฟส และคีย์การเข้าถึง เพื่อให้มั่นใจว่าผู้ใช้แต่ละคนสามารถเข้าถึงทรัพยากรคอม พิวเตอร์คลาวด์ที่ตนซื้อได้เท่านั้น ซึ่งทำให้เกิดการแยกการเข้าถึงระหว่างผู้เช่าหลายรายได้ อย่างมีประสิทธิภาพ การจัดการความต่อเนื่องของธุรกิจ: Tencent Cloud ได้รับการรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจ เพื่อให้มั่นใจในความต่อเนื่องและความพร้อมใช้งานของธุ รกิจลูกค้า Tencent Cloud ได้จัดทำแผนกู้คืนจากภัยพิบัติโดยละเอียดสำหรับผลิตภัณฑ์ คลาวด์ของตน และดำเนินการฝึกซ้อมตามแผนกู้คืนจากภัยพิบัตินั้นอย่าง เคร่งครัดตามข้อกำหนด เพื่อรับประกันความทันเวลาความเป็นไปได้ของแผนกู้คืน จากภัยพิบัติ การปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ และมาตรฐานแห่งชาติ: Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจ ศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ได้รับการรับรองและคุณวุฒิด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวหลายรายการผ่านการตรวจสอบหรือประเมินโดยบุคคลที่สามที่เป็นอิสระ เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, SOC ซึ่งพิสูจน์ว่าความสามารถด้านความปลอดภัยและการปกป้องความเป็นส่วนตัวของ Tencent Cloud เป็นไปตามมาตรฐานการรับรองที่เกี่ยวข้องหรือแนวปฏิบัติที่ดีของอุตสาหกรรม และได้รับการตรวจสอบจากสถาบันตรวจสอบบุคคลที่สามมีอาชีพเป็นประจำทุกปี ปัจจัยภายนอกที่เกิดจากประเทศที่บุคคลที่สามตั้งอยู่: โครงสร้างพื้นฐานของ Tencent Cloud ครอบคลุมหลายพื้นที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) โดยแต่ละภูมิภาคเป็นพื้นที่ทางภูมิศาสตร์ที่แยกอิสระ และแต่ละโซนความพร้อมใช้งานเป็นโดเมนการบำรุงรักษาและรับมือเหตุขัดข้องที่แยกจากกัน โซนความพร้อมใช้งานแต่ละแห่งถูกแยกทางกายภาพ ลูกค้าสามารถวางระบบและจัดเก็บข้อมูลบนภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระตามความต้องการในการขยายธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อรับประกันความต้องการด้านการรับมือเหตุขัดข้องของธุรกิจ ภายในปี 2026 Tencent Cloud ได้ดำเนินการติดตั้งศูนย์ข้อมูลสามแห่งในประเทศไทย โดยศูนย์ข้อมูลแต่ละแห่งมีการจัดการด้านไฟฟ้าและเครือข่ายที่เป็นอิสระต่อกัน เพื่อรองรับการจัดเก็บ ประมวลผล และสำรองข้อมูลของลูกค้าภายในประเทศได้อย่างมีประสิทธิภาพ การทำงานร่วมกันได้: หากลูกค้าจำเป็นต้องยกเลิกข้อตกลงตามสัญญาเนื่องจากมีการเปลี่ยนแปลงธุรกิจหรือการวางแผนเทคโนโลยีสารสนเทศในอนาคต ลูกค้าสามารถเลือกทำการสำรองข้อมูลและย้ายข้อมูลและสภาพแวดล้อมการผลิตบนคลาวด์ได้ทุกเวลา ผลิตภัณฑ์คลาวด์ที่ Tencent Cloud ให้มารองรับให้ลูกค้าใช้รูปแบบมาตรฐานทั่วไปเพื่อสำรอง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และย้ายข้อมูลของลูกค้า และลูกค้าสามารถใช้วิธีการส่งและโปรโตคอลการส่งเดียวกันกับขั้นตอนการย้ายขึ้นคลาวด์ หรือใช้บริการเครือข่าย เช่น Direct Connect (DC) VPN Connection เพื่อให้มั่นใจว่าข้อมูลของลูกค้าในขั้นตอนการย้ายออกจากคลาวด์มีความปลอดภัยและเชื่อถือได้
9	การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเปิดเผย สัญญา และจัดเก็บสัญญา การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก	9.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเปิดเผย สัญญา และจัดเก็บสัญญา หรือข้อตกลงดังกล่าวไว้ที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจเพื่อสามารถบังคับใช้ได้ตามกฎหมาย 9.2 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญในสัญญา หรือข้อตกลงกับบุคคลภายนอกอย่างชัดเจน โดยพิจารณาให้ครอบคลุมตามขอบเขต ระดับความ เสี่ยงและความมีนัยสำคัญของการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจาก	ลูกค้าควรทำสัญญาการจ้างทำภายนอก (Outsourcing Agreement) กับผู้ให้บริการ ซึ่งครอบคลุมขอบเขตของข้อตกลงการจ้างทำภายนอกหน้าที่และความรับผิดชอบของทั้งสองฝ่าย มาตรฐานการให้บริการ ความต่อเนื่องทางธุรกิจ การรายงานเหตุการณ์สำคัญ กลไกการตรวจสอบและควบคุม การทบทวน การแจ้งเหตุการณ์ที่ไม่พึงประสงค์ การรับข้อพิพาท การยุติสัญญาเนื่องจากผิดนัดและการถอนตัวล่วงหน้า กฎหมายที่ใช้บังคับ และเนื้อหาอื่นๆ และต้องมั่นใจว่าสัญญามีความถูกต้องตามกฎหมายและสามารถบังคับใช้ได้ Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสองฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้
10	การติดตามผลการปฏิบัติงานของบุคคลภายนอก	10.1 สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดผู้รับผิดชอบและติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจาก	ลูกค้าควรติดตามการปฏิบัติตามข้อตกลงของบุคคลที่ตามมาอย่างต่อเนื่อง และกำหนดให้บุคคลที่สามารถรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างกระบวนการดำเนินงานอย่างทันท่วงที นอกจากนี้ ลูกค้าควรประเมินความร่วมมือกับบุคคลที่สามที่ดำเนินอยู่ใหม่ก่อนการต่ออายุสัญญาหรือตามรอบระยะเวลาที่กำหนด

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		บุคคลภายนอก เช่น กำหนดให้บุคคลภายนอก รายงานผลการปฏิบัติงานอย่างสม่ำเสมอ กำหนดการประชุมติดตามอย่างสม่ำเสมอและต่อเนื่อง การเข้าถึงเหตุการณ์การดำเนินงานของบุคคลภายนอก เป็นต้น 10.2สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดให้บุคคลภายนอกรายงานเหตุการณ์ ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องให้สถาบันการเงินและสถาบันการเงินเฉพาะ กิจได้รับทราบอย่างทันการณเพื่อประเมินผลกระทบที่มีต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ทั้งนี้กรณีประเมินว่าผลกระทบที่เกิดขึ้นมีผลต่อการดำเนินธุรกิจของสถาบันการเงินและสถาบัน การเงินเฉพาะกิจอย่างมีนัยสำคัญ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีส่วนร่วม ในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ 10.3สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรทบทวนการประเมินศักยภาพ การประเมินผลการปฏิบัติงาน และการประเมินความเสี่ยงของการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจาก บุคคลภายนอกทั้งในด้านประสิทธิภาพการรักษาความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศ และการปฏิบัติตามกฎหมาย เมื่อจะต่อสัญญาและเมื่อถึงรอบระยะเวลาที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจกำหนด ทั้งนี้ การใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล	หนด (อย่างน้อยปีละหนึ่งครั้ง) เพื่อสนับสนุนข้อกำหนดการตรวจสอบบุคคลที่สามของลูกค้า Tencent Cloud จะให้ความร่วมมือตามสถานการณ์จริงและตามข้อตกลงที่ตกลงกับลูกค้า ในการตรวจสอบความปลอดภัยและการกำกับดูแลของบุคคลที่สามของลูกค้า และจัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบที่ลูกค้าเป็นผู้ริเริ่มอย่างเข้มข้น บริการคลาวด์ที่ Tencent Cloud มอบให้แก่ลูกค้ามีการส่งมอบตามข้อตกลงระดับการให้บริการ (SLA) ที่ตกลงกันสำหรับแต่ละบริการ ตัวชี้วัดประสิทธิภาพ เกณฑ์การวัด และข้อกำหนดในการรายงานสำหรับบริการแต่ละรายการ กำหนดไว้อย่างชัดเจนใน SLA ของผลิตภัณฑ์แต่ละรายการ และเผยแพร่บนเว็บไซต์อย่างเป็นทางการของ Tencent Cloud Tencent Cloud จะติดตามประสิทธิภาพและความพร้อมใช้งานของบริการคลาวด์อย่างต่อเนื่อง และให้การตรวจสอบแบบเรียลไทม์แก่ลูกค้าผ่านคอนโซลการจัดการ นอกจากนี้ ปัจจุบัน Tencent Cloud ได้รับการรับรองและคุณวุฒิด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดความเป็นส่วนตัวหลายรายการผ่านการตรวจสอบหรือการประเมินโดยบุคคลที่สามที่เป็นอิสระ และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่หน่วยงานผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่นๆ ที่เกี่ยวข้อง สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ต่อความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
11	การยกเลิกและ การสิ้นสุดส ัญญาหรือข้อ ตกลง	จากบุคคลภายนอกที่มีนัยสำคัญ ควรกำหนดให้ดำเนินการอย่างน้อย ปีละครั้ง รวมถึงให้รายงานผลการประเมินดังกล่าวต่อ คณะกรรมการหรือผู้บริหารระดับสูง ที่ได้รับมอบหมาย	และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้ เหลือน้อยที่สุด
		11.1 จัดให้มีมาตรฐานหรือระเบียบป ฏิบัติว่าด้วยการยกเลิกและสิ้นสุดส ัญญาหรือข้อตกลง เพื่อเป็น กรอบแนวทางการยกเลิกหรือสิ้นสุด สัญญาหรือข้อตกลง โดยคำนึงถึงความต่อเนื่องในการให้ บริการ และความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ทั้งนี้ มาตรฐานหรือระเบียบปฏิบัติดังกล่าว ควรครอบคลุม บทบาทหน้าที่คณะกรรมการและหน วยงานที่เกี่ยวข้องกระบวนการและก ารควบคุมภายใน 11.2 การพิจารณายกเลิกหรือสิ้นสุด สัญญาหรือข้อตกลง สถาบันการเงินและสถาบันการเงินเ นเฉพาะกิจ ควรประเมินผลกระทบและความเสี ยที่อาจเกิดขึ้นจากการยกเลิกและส ิ้นสุดสัญญาหรือข้อตกลง และดำเนินการตามมาตรฐานหรือระ เบียบปฏิบัติว่าด้วยการยกเลิกและส ิ้นสุดสัญญาหรือข้อตกลง และ กำหนดกลยุทธ์และแผนงานการยกเลิกและสิ้นสุดสัญญาหรือข้อตกลง (exit strategy and exit plan) ที่ชัดเจน เพื่อให้มั่นใจว่าการยกเลิกหรือสิ้นสุด สัญญาหรือข้อตกลงเป็นไปอย่างมี ประสิทธิภาพและได้เตรียมความพร ้อมต่อผลกระทบที่อาจเกิดขึ้น เช่น การหยุดให้บริการของระบบที่ ส่งผลกระทบกับลูกค้าหรือผู้บริก	ลูกค้าควรกำหนดขั้นตอนการยกเลิกหรือสิ้นสุดสัญญา หรือข้อตกลง กำหนดกลยุทธ์และแผนการยุติการให้บริการให้ชัดเจน เพื่อให้มั่นใจในความพร้อมใช้งานของธุรกิจระหว่างกระบวนการยกเลิกหรือสิ้นสุด หากลูกค้าจำเป็นต้องยกเลิกข้อตกลงตามสัญญาเนื่องจาก มีการเปลี่ยนแปลงธุรกิจหรือการวางแผนเทคโนโลยีสารสนเทศในอนาคต ลูกค้าสามารถเลือกทำการสำรองข้อมูลและย้ายข้อมูลแล ะสภาพแวดล้อมการผลิตบนคลาวด์ได้ทุกเวลา ผลิตภัณฑ์คลาวด์ที่ ตามข้อตกลงการให้บริการระหว่าง Tencent Cloud กับลูกค้า หากบริการคลาวด์หมดอายุหรือสิ้นสุดลง สำหรับข้อมูลที่ลูกค้าเก็บไว้ในเซิร์ฟเวอร์คลาวด์เนื่องจากการใช้บริการ Tencent Cloud ลูกค้าจำเป็นต้องทำการย้ายข้อมูลให้เสร็จสิ้นก่อนช่วงเวลา กักเก็บข้อมูลสิ้นสุดลง Tencent Cloud ให้มารองรับให้ลูกค้าใช้รูปแบบมาตรฐานทั่วไปเพื่อสำรอง และย้ายข้อมูลของลูกค้า และลูกค้าสามารถใช้วิธีการส่งและโปรโตคอลการส่งเดียวกันกับขั้นตอนการย้ายขึ้นคลาวด์ หรือใช้บริการเครือข่าย เช่น Direct Connect (DC) VPN Connection เพื่อให้มั่นใจว่าข้อมูลของลูกค้าในขั้นตอนการย้ายออกจาก คลาวด์มีความปลอดภัยและเชื่อถือได้ เมื่อบริการคลาวด์สิ้นสุดลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยจะลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรอง อย่างสิ้นเชิงหลังจากช่วงเวลากักเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		าร การรักษาความมั่นคงปลอดภัยด้าน เทคโนโลยีสารสนเทศ เป็น ต้น	
12.1	การจัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง	จัดให้มีหน่วยงานผู้รับผิดชอบในการ จัดทำ และปรับปรุงทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยี สารสนเทศที่เกี่ยวข้อง เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถนำมาใช้ระบุ ความเสี่ยงได้ อย่างชัดเจน และสามารถบริหารจัดการทรัพย์สิน ด้านเทคโนโลยีสารสนเทศได้อย่างปลอดภัย และทันการณ์	ลูกค้าควรบำรุงรักษาบัญชีรายการสินทรัพย์ที่ประกอบด้วย บริการภายนอก การเชื่อมต่อหรือการเข้าถึงข้อมูลและสินทรัพย์ข้อมูลที่เกี่ยวข้อง และสร้างกลไกการจัดการสินทรัพย์ข้อมูลเพื่อระบุสินทรัพย์ จัดระดับและหมวดหมู่ กำหนดกรรมสิทธิ์ในสินทรัพย์ และจัดการความปลอดภัยของสินทรัพย์ตามระดับที่แตกต่าง กัน บัญชีรายการสินทรัพย์ควรได้รับการทบทวนเป็นประจำ และควรได้รับการปรับปรุงให้ทันสมัยทันทีเมื่อมีการเปลี่ยนแปลง เพื่อช่วยเหลือลูกค้าในการบริหารสินทรัพย์ข้อมูลอย่างครอบคลุม Tencent Cloud Cloud Workload Protection Platform (CWPP) ซึ่งสนับสนุนการรวบรวมลายเซ็นดิจิทัลของสินทรัพย์โดยอัตโนมัติ และบริหารจัดการข้อมูลลายเซ็นดิจิทัลของสินทรัพย์ เช่น บัญชีผู้ใช้ พอร์ต กระบวนการ และแอปพลิเคชัน อย่างเป็นเอกภาพ CWPP ยังสามารถดำเนินการตรวจสอบอย่างรวดเร็วเกี่ยวกับขอบเขตผลกระทบความเสี่ยงของเหตุการณ์ความปลอดภัยที่เกิดขึ้นแล้ว ตามลายเซ็นดิจิทัลของสินทรัพย์ เพื่อช่วยลูกค้ายกระดับความปลอดภัยของเซิร์ฟเวอร์ ลูกค้ายังสามารถใช้แพลตฟอร์มการจัดการความปลอดภัยแบบครบวงจร Cloud Security Center (CSC) ของ Tencent Cloud เพื่อบริหารจัดการความปลอดภัยของสินทรัพย์ข้อมูล CSC มีฟังก์ชันศูนย์ความปลอดภัยสินทรัพย์ ซึ่งช่วยให้ลูกค้าสามารถตรวจนับสินทรัพย์บนคลาวด์แบบไดนามิกโดยอัตโนมัติ รวมถึงเซิร์ฟเวอร์คลาวด์ ที่เก็บวัตถุ ฐานข้อมูลคลาวด์ โหลดบาลานเซอร์ เป็นต้น และบริหารจัดการความเสี่ยงด้านความปลอดภัยของสินทรัพย์แบบครบวงจรผ่านหลายมิติความปลอดภัย เช่น ความเสี่ยงการกำหนดค่าคลาวด์ ช่องโหว่ และเหตุการณ์ความปลอดภัย เพื่อลดความเสี่ยง "IT ล่องหน" บนคลาวด์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ได้กำหนดมาตรฐานการจัดการสินทรัพย์ข้อมูลและกระบวนการจัดการตลอดวงจรชีวิตสินทรัพย์ เพื่อจัดการและปกป้องสินทรัพย์ เช่น ข้อมูลอิเล็กทรอนิกส์ ฮาร์ดแวร์และอุปกรณ์เสมือน โครงสร้างพื้นฐาน ระบบแอปพลิเคชัน และซอฟต์แวร์ โดยจำแนกประเภทและระดับ Tencent Cloud ใช้ระบบการจัดการสินทรัพย์ในการบริหารจัดการอุปกรณ์ฮาร์ดแวร์และส่วนประกอบซอฟต์แวร์ รวมถึงการลงทะเบียนและผูกมัดสินทรัพย์ การตรวจนับและการอัปเดตข้อมูลสินทรัพย์ การปลดระวางและเปลี่ยนใหม่สินทรัพย์ เป็นต้น เพื่อรับประกันการทำงานที่ราบรื่นของระบบพื้นฐานของแพลตฟอร์มคลาวด์ และจัดเตรียมการสนับสนุนที่เชื่อถือได้ให้กับระบบธุรกิจ
12.2	การรักษาความมั่นคงปลอดภัยของข้อมูล	(1)ดูแลข้อมูลที่อยู่ภายใต้การดูแลของบุคคลภายนอกให้เป็นไปตามนโยบายและมาตรฐานของสถาบันการเงินและสถาบันการเงินเฉพาะกิจสอดคล้องกับมาตรฐานสากลตามระดับชั้นของ ข้อมูล (informationclassification) ครอบคลุมทั้งข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (data at endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย(data in transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (data at rest) ซึ่งรวมถึงข้อมูลที่ถูกจัดเก็บที่สื่อบันทึก ข้อมูลสำรอง (2)บริหารจัดการกุญแจและการเข้ารหัสข้อมูลด้วยตนเอง ซึ่งการควบคุมในทุกขั้นตอนตลอดวงจรการบริหารจัดการกุญแจและการเข้ารหัส (lifecycle of cryptographic keys) ตั้งแต่การสร้าง การ จัดเก็บ การใช้งาน การสำรอง การเพิกถอน และการต่ออายุของกุญแจเข้ารหัสข้อมูล	ลูกค้าควรกำหนดกลไกการปกป้องความปลอดภัยของข้อมูล เพื่อให้มั่นใจว่าข้อมูลที่หน่วยงานภายนอกเก็บรักษาอยู่นั้นได้รับการจำแนกประเภทตามระดับความอ่อนไหวและความสำคัญของข้อมูลตามกลไกความปลอดภัยข้อมูลภายในของลูกค้า และดำเนินมาตรการป้องกันข้อมูลตามระดับข้อมูลที่แตกต่างกัน ใช้มาตรฐานการเข้ารหัสที่เชื่อถือได้และเป็นที่ยอมรับในระดับสากล เพื่อปกป้องความเป็นความลับและความสมบูรณ์ของข้อมูล นอกจากนี้ ลูกค้ายังควรควบคุมวงจรชีวิตของคีย์ลับ (คีย์การเข้ารหัส) อย่างเข้มงวด หากลูกค้าใช้คีย์การเข้ารหัสของหน่วยงานภายนอก ต้องให้ความสนใจในความปลอดภัยของคีย์การเข้ารหัสดังกล่าว ในด้านการจำแนกประเภทและระดับข้อมูล Data Security Governance Center (DSGC) สามารถช่วยลูกค้าจัดการสินทรัพย์ข้อมูลโดยอัตโนมัติ จัดประเภทและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลขององค์กรบนคลาวด์ โดยได้รับอนุญาตจากองค์กร DSGC จะเชื่อมต่อกับสินทรัพย์ข้อมูลประเภทต่างๆ บนคลาวด์อย่างลึกซึ้ง และรับข้อมูลสินทรัพย์ข้อมูลทีละเวลาจากมิติภายในตามลักษณะของข้อมูล DSGC จะช่วยองค์กรค้นพบข้อมูลที่ละเอียดอ่อนอย่างเจาะจง และจัดระเบียบสินทรัพย์ข้อมูลจากมุมมองความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		(3)สร้างกฎแฉการเข้ารหัสข้อมูลด้วยตนเอง ทั้งนี้ หากสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ไม่สามารถสร้างกฎแฉการเข้ารหัสด้วยตนเองได้สถาบันการเงินและสถาบันการเงินเฉพาะกิจ ควรมั่นใจได้ว่ากฎแฉการเข้ารหัสของบุคคลภายนอกไม่มีการนำมาใช้ร่วมกับผู้ใช้บริการรายอื่น และทราบถึงรายละเอียดเกี่ยวกับระบบการบริหารจัดการกฎแฉการเข้ารหัสข้อมูลของ	ตามมาตรฐานการจำแนกประเภทและระดับข้อมูลระดับชาติ อุตสาหกรรม หรือองค์กร DSGC จะช่วยองค์กรในการจำแนกประเภทและระดับข้อมูล
		(4)เก็บกฎแฉการเข้ารหัสข้อมูลในอุปกรณ์รักษาความปลอดภัย เช่น hardware security module (HSM) เป็นต้น และดูแลรักษาความปลอดภัยอุปกรณ์ HSM ด้วยการจัดตั้งในโซนเครือข่ายที่ปลอดภัยและจำกัดการเชื่อมต่อกับระบบงานอื่นที่ไม่เกี่ยวข้อง	ในด้านการป้องกันการจัดเก็บข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูลโดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสานรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล
		(5)สอบทานการปฏิบัติงานการบริหารจัดการการเข้ารหัสข้อมูลทั้งที่ดำเนินการเองและดำเนินการโดยบุคคลภายนอก ให้ครอบคลุมการสอบทานช่องโหว่และความเสี่ยงของการเข้ารหัสข้อมูล โดยพิจารณาให้มีความปลอดภัยสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป เช่น อัลกอริธึมการเข้ารหัส (encryption algorithm) และขนาดความยาวของกฎแฉการเข้ารหัส ข้อมูล เป็นต้น	ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้านบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เน็ต Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจก็มีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า
			เพื่อช่วยลูกค้าในการปกป้องความเป็นความลับ ความสมบูรณ์ และความพร้อมใช้งานของคีย์ลับ ลูกค้าสามารถใช้ Key Management Service (KMS) ได้ KMS รองรับให้ลูกค้าสร้างและจัดการคีย์ได้อย่างง่ายดาย ตอบสนองความต้องการในการจัดการคีย์สำหรับแอปพลิเคชันและธุรกิจหลายรายการของลูกค้า และสอดคล้องกับข้อกำหนดด้านกฎระเบียบและการปฏิบัติตามข้อกำหนด ระบบการจัดการคีย์ใช้ Hardware Security Module (HSM) ที่ได้รับการรับรอง FIPS-140-2 ในการสร้างและปกป้องคีย์ ใช้โปรโตคอลการส่งข้อมูลที่ปลอดภัย ใช้การปรับใช้ธุรกิจแบบกระจายคลัสเตอร์หลายศูนย์ข้อมูลและการสำรองข้อมูลออนไลน์ อุปกรณ์ HSM ชั้นล่างใช้การปรับใช้การสำรองข้อมูลแบบออฟไลน์ในศูนย์ข้อมูลสองแห่ง เพื่อให้มั่นใจในความพร้อมใช้งานสูงของระบบการจัดการคีย์
			เพื่อรับประกันความปลอดภัยของข้อมูลที่ถูกเข้ารหัสและลดความเสี่ยงจากการถูกโจมตีหรือใช้ในทางที่ผิดของคีย์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			KMS รองรับการหมุนเวียนคีย์เป็นระยะ และหลังการหมุนเวียนคีย์จะยังคงเข้ากันได้กับข้อมูลที่ถูกเ เข้ารหัสก่อนการหมุนเวียน โดยไม่ส่งผลกระทบต่อการทำงานของธุรกิจผู้ใช้ KMS ใช้วิธีการลบคีย์ที่หมดอายุ ถูกยกเลิก หรือรั่วไหลออกไปอย่างปลอดภัยและเชื่อถือได้ คีย์ที่ถูกลบไปแล้วไม่สามารถกู้คืนได้ และข้อมูลที่ถูกเข้ารหัสด้วยคีย์ดังกล่าวก็จะไม่สามารถถอ รหัสได้เช่นกัน สำหรับสถาบันในภาคการเงินที่ข้อมูลการสื่อสารและการ จัดเก็บมีมูลค่าสูงและมีความลับสูง KMS ให้บริการการเข้ารหัส การปกป้องคีย์ และการจัดการสิทธิ์สำหรับเนื้อหาการสื่อสารตามข้อตกล ง ไฟล์สำคัญ และข้อมูลสำคัญผ่านการเข้ารหัสแบบซองจดหมาย (envelope encryption) เพื่อให้เป็นไปตามข้อกำหนดด้านความปลอดภัยและการป ฏิบัติตาม กระบวนการส่งและกระจายคีย์ได้รับการปกป้องด้วยการเ เข้ารหัส โดยเปิดใช้งาน TLSv1.2 เพื่อป้องกันการดักจับและการขโมยข้อมูลโดยบุคคลที่สาม (man-in-the-middle attacks) ในด้านการจัดการคีย์ Tencent Cloud ยังได้กำหนดมาตรฐานการเข้ารหัสและการจัดการคีย์ โดยกำหนดข้อกำหนดด้านความปลอดภัยสำหรับกระบวน การต่างๆ ในการสมัครคีย์ การสร้าง การจัดเก็บ การใช้ การส่งต่อ การอัปเดต และการทำลายคีย์ การดำเนินการต่างๆ ที่เกี่ยวข้องกับวงจรชีวิตของคีย์ทั้งหมดต้องปฏิบัติตามข้อ กำหนดพื้นฐานของการควบคุมสองชั้น การส่งมอบที่เข้มงวด การเก็บรักษาที่เหมาะสม และการอัปเดตที่ทันเวลา กระบวนการใช้คีย์ยังต้องแน่ใจว่าปฏิบัติตามข้อกำหนด เช่น การแยกหน้าที่และความรับผิดชอบ การอนุมัติที่เข้มงวด และการดำเนินการด้วยชื่อจริง และต้องเก็บรักษาบันทึกการดำเนินการคีย์ทางธุรกิจ และดำเนินการตรวจสอบการดำเนินการเป็นประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความปลอดภัยข้อมูล โปรดดูเนื้อหาในข้อ "2 การรักษาความมั่นคงปลอดภัยของข้อมูล ของ "5.3 เอกสารแนบ 2"

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
12.3	การควบคุมการเข้าถึง	(1) กำหนดกระบวนการจัดการและควบคุมดูแลสิทธิในการเปิดใช้และการเข้าถึงระบบและข้อมูล ที่ชัดเจนเป็นลายลักษณ์อักษร เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่กำหนด สอดคล้องตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป (2) กำหนดบทบาทหน้าที่และความรับผิดชอบของผู้มีสิทธิใช้งานระบบและผู้ใช้งานที่ได้รับสิทธิสูงให้ชัดเจน (3) ควบคุมดูแลการให้สิทธิแก่บุคคลภายนอก โดยจำกัดสิทธิตามบทบาทหน้าที่และความจำเป็นในการใช้งาน มีการอนุมัติการเปิดใช้งานเพื่อไม่ให้บุคคลใดบุคคลหนึ่งปฏิบัติงานได้ ตั้งแต่ต้น จนจบกระบวนการ (4) มีระบบหรือกระบวนการติดตามระหว่างการใช้งานบัญชีผู้ใช้งานที่มีสิทธิสูงสุด รวมทั้ง ควรติดตามและสอบถามสถานะสิทธิและการใช้งานหรือการเข้าถึงระบบข้อมูล ตามรอบ ระยะเวลาที่สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิอย่างเป็นประจำ เพื่อให้มั่นใจว่า การใช้งานสิทธิเป็นไปตามขอบเขตและความจำเป็นในการใช้งาน (5) กำหนดวิธีการระบุและพิสูจน์ตัวตนผู้ใช้งาน ด้วยวิธีการที่รัดกุมเพียงพอ สอดคล้องกับ มาตรฐานนโยบายที่สถาบันการเงิน	ลูกค้าควรสร้างกลไกการพิสูจน์ตัวตนและความคุมการเข้าถึงสำหรับข้อมูลและระบบเทคโนโลยีสารสนเทศเพื่อควบคุมการเข้าถึงสินทรัพย์ข้อมูล บทบาทและอัปเดตสิทธิเป็นประจำ และเสริมสร้างการจัดการความปลอดภัยของบัญชีผู้ใช้ที่มีสิทธิพิเศษโดยใช้การพิสูจน์ตัวตนหลายปัจจัยและกลไกการตรวจสอบ นอกจากนี้ ลูกค้ายังควรสร้างกลไกการจัดการการเข้าถึงระยะไกลที่ปลอดภัย ในด้านการจัดการบัญชีผู้ใช้และการให้สิทธิ Cloud Access Management (CAM) สามารถช่วยลูกค้าจัดการการเข้าถึงผลิตภัณฑ์และบริการของ Tencent Cloud ได้อย่างปลอดภัยและละเอียดรอบคอบ Tencent Cloud ยังได้กำหนดกลยุทธ์การให้สิทธิการควบคุมการเข้าถึงและกลไกเมทริกซ์การแบ่งแยกสิทธิภายในองค์กร Tencent Cloud ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการตรวจสอบสิทธิการเข้าถึงของพนักงาน โดยผู้ใช้ต้องผ่านการยืนยันตัวตนสองปัจจัยก่อนเข้าถึงทรัพยากรภายใน Tencent Cloud ปฏิบัติตามหลักการสิทธิที่น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิที่น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิเฉพาะก็ต่อเมื่อมีความจำเป็นต้องใช้และผ่านกระบวนการอนุมัติสิทธิที่เข้มงวดเท่านั้น Tencent Cloud จะรักษามั่นทึกข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบทบาทหน้าที่และระดับสิทธิในระบบธุรกิจต่างๆ และด้วยการจัดงานตรวจสอบสิทธิภายในเป็นประจำเพื่อให้มั่นใจว่าสิทธิจะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์ สำหรับผู้ที่มีสิทธิสูง Tencent Cloud มี Bastion Host (BH) ที่สามารถรองรับการให้สิทธิอย่างละเอียดตามมิติต่างๆ เช่น ผู้ใช้ สินทรัพย์ บัญชี และสิทธิการดำเนินงาน เพื่อให้มั่นใจว่าสิทธิที่ผู้ใช้มีอยู่เป็นสิทธิขั้นต่ำที่จำเป็นสำหรับ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		และสถาบันการเงินเฉพาะกิจกำหนด หรือมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป	รับการเข้าถึงสินทรัพย์และทำงานให้สำเร็จ สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้ เครื่องบินคู่กัน อย่างเต็มรูปแบบ
	(6) ในกรณีที่บุคคลภายนอกเชื่อมต่อเพื่อเข้าถึงระบบงานของสถาบันการเงินและสถาบันการเงินเฉพาะกิจผ่านช่องทางการเข้าถึงระบบงานระยะไกล (system remote access) สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีกระบวนการบริหารจัดการการเข้าถึงระยะไกลด้วยวิธีการที่ปลอดภัย		โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบและบิกเอนด์จากส่วนกลางผ่าน เครื่องบินคู่กัน การเข้าถึง เครื่องบินคู่กัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติสิทธิ์ มีเฉพาะเจ้าหน้าที่ปฏิบัติการภายในของ Tencent Cloud บางส่วนเท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบ เครื่องบินคู่กัน ต้องการการยืนยันตัวตนสองปัจจัย
	(7) ดูแลให้บุคคลภายนอกจัดเก็บบันทึกข้อมูลประวัติของการพิสูจน์ตัวตนและการเข้าถึง (access log) บันทึกการดำเนินงาน (activity log) ตามระยะเวลาที่กฎหมายกำหนด โดยมีการสอบทานข้อมูลการบันทึกเหตุการณ์ตามรอบระยะเวลาที่สอดคล้องกับความเสี่ยงและความสำคัญอย่างเป็นประจำ เพื่อให้มั่นใจว่าบุคคลภายนอกปฏิบัติงานเป็นไปตามข้อตกลงและมาตรฐานการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ		ในด้านการเฝ้าระวังความปลอดภัยของบัญชี Cloud Access Management (CAM) ผ่านฟังก์ชันการควบคุมสิทธิ์อย่างละเอียดอ่อน มอบสิทธิ์เฉพาะให้กับบุคคลากรต่างๆ สำหรับทรัพยากรที่แตกต่างกัน ลูกค้ายังสามารถดูและติดตามบันทึกการดำเนินการของพนักงานผ่าน CloudAudit รองรับการดูบันทึกการดำเนินการของคอนโซล Tencent Cloud และ API คลาวด์ภายใน 90 วันออนไลน์ Tencent Cloud ยังให้บริการ Bastion Host (BH) ซึ่งรองรับฟังก์ชันการตรวจสอบการดำเนินการ โดยบันทึกและวิเคราะห์บันทึกการดำเนินการของผู้ใช้ เพื่อให้แน่ใจว่าสามารถติดตามเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพ เพื่อสนับสนุนลูกค้าในการปฏิบัติตามข้อกำหนดทางกฎระเบียบ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยสถานะการเข้าสู่ระบบบัญชีพนักงานแบบเรียลไทม์ ทันทีที่ตรวจพบพฤติกรรมกรรมการเข้าสู่ระบบที่ผิดปกติใดๆ ระบบจะติดต่อเจ้าของบัญชีทันทีเพื่อดำเนินการตรวจสอบและจัดการ และบันทึกเหตุการณ์ที่เกี่ยวข้องอย่างละเอียด สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้ เครื่องบินคู่กัน อย่างเต็มที่ การดำเนินการที่ละเอียดอ่อนในสภาพแวดล้อมการผลิตทั้งหมดต้องเข้าถึงผ่านการเข้าสู่ระบบ เครื่องบินคู่กันแบบเรียลไทม์ และบันทึกการเข้าสู่ระบบและบันทึกการดำเนินการทั้งหมดจะถูกรวบรวมไปยังแพลตฟอร์มการจัดการบันทึก (log)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ของ Tencent Cloud เพื่อเก็บรักษาในรูปแบบเข้ารหัสผ่านเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติการและหิมตรวจสอบภายในจะทำการตรวจสอบบันทึก (log) เพื่อตรวจจับความผิดปกติของระบบหรือการดำเนินการเพื่อป้องกันความเสี่ยงในการปฏิบัติการ สำหรับการเข้าถึงระยะไกล เพื่อความสะดวกของลูกค้าในการเข้าถึงระบบธุรกิจบนคลาวด์ได้อย่างปลอดภัยและรวดเร็ว ทุกเวลา ทุกสถานที่ และโดยใช้อุปกรณ์ปลายทางหลักใดๆ ก็ตาม Tencent Cloud รองรับเทคโนโลยีการเข้าถึงระยะไกล SSL VPN SSL VPN สามารถปกป้องความปลอดภัยของข้อมูลที่ส่งผ่านอินเทอร์เน็ตด้วยวิธีการเข้ารหัส และยังรองรับการควบคุมการเข้าถึงที่เหมาะสมเพื่อลดการเข้าถึงโดยไม่ได้รับอนุญาต ลูกค้ายังสามารถใช้ VPN Connection เพื่อให้บรรลุการส่งข้อมูลระหว่างศูนย์ข้อมูลในพื้นที่และทรัพยากรบน Tencent Cloud ฝั่ง VPN ใช้ IKE (โปรโตคอลแลกเปลี่ยนคีย์ลับ) และ IPsec เพื่อเข้ารหัสข้อมูลที่ส่ง สร้างฝั่งข้อมูลที่ปลอดภัยและนำเชื่อมกับอินเทอร์เน็ต เพื่อปกป้องความปลอดภัยของข้อมูลระหว่างการส่ง VPN Gateway มีความน่าเชื่อถือสูง โดยใช้สถาปัตยกรรมการสำรองข้อมูลออนไลน์แบบสองเครื่องที่ระดับล่าง เพื่อรับประกันว่าการสื่อสารเซชันจะไม่ขาดตอนและแอปพลิเคชันระดับบนไม่รู้สึกถึงเปลี่ยนแปลง Tencent Cloud ได้สร้างขั้นตอนการจัดการการเข้าถึงระยะไกลของพนักงานภายใน โดยพนักงานสามารถใช้อุปกรณ์ที่เชื่อถือได้ซึ่งลงทะเบียนกับ Tencent Cloud แล้วเท่านั้น และเข้าถึงเครือข่ายสำนักงานและระบบงานประจำวันของ Tencent Cloud ทางไกลผ่านช่องทางการสื่อสารที่เข้ารหัส Tencent Cloud จะบำรุงรักษาบันทึกการเข้าถึงระยะไกลและบันทึกพฤติกรรมดำเนินการของผู้ใช้ ในเวลาเดียวกัน เครือข่ายสำนักงานภายในของ Tencent Cloud และสภาพแวดล้อมการผลิตที่ข้อมูลลูกค้าอยู่นั้นถูกแยกจ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ากกันโดยสมบูรณ์ เมื่อพนักงานของ Tencent Cloud ได้รับความยินยอมและการอนุญาตจากลูกค้าให้เข้าถึงสินทรัพย์ข้อมูลของลูกค้า ต้องเข้าถึงสภาพแวดล้อมการผลิตที่ข้อมูลลูกค้าอยู่ผ่านเครื่องบินคัมกัน และบัญชีการปฏิบัติงานทั้งหมดมีการติดตั้งกลไกการยืนยันตัวตนสองปัจจัย เมื่อให้สิทธิ์ Tencent Cloud ใช้การแบ่งสิทธิ์ที่ละเอียดเพื่อให้มั่นใจว่าจะให้สิทธิ์เฉพาะสิทธิ์ขั้นต่ำที่จำเป็นสำหรับพนักงานในการให้บริการที่เกี่ยวข้องเท่านั้น การขอสิทธิ์เพิ่มเติมทั้งหมดต้องผ่านการทบทวนและอนุมัติหลายระดับ และบันทึกการดำเนินการแบ็กเอนด์ทั้งหมดจะถูกเก็บไว้โดยศูนย์กลางแพลตฟอร์มบันทึก (log) และได้รับการตรวจสอบโดยทีมตรวจสอบภายในของ Tencent Cloud เป็นประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมการเข้าถึงโปรดดูเนื้อหาในข้อ "3.1, 3.2 การควบคุมการเข้าถึง ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ในคู่มือนี้
12.4	การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร	(1)รักษาความปลอดภัยในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารกับบุคคลภายนอกเป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศรวมทั้งตามมาตรฐานสากลที่ยอมรับโดยทั่วไป (2)ดูแลให้บุคคลภายนอกมีระบบหรือกระบวนการสำหรับคัดกรอง traffic ที่ส่งผ่านระบบเครือข่าย ตรวจสอบ แจ้งเตือน และสามารถยับยั้งการบุกรุกหรือตอบโต้การโจมตีได้โดยอัตโนมัติ แบบต่อเนื่องบนระบบเครือข่ายให้เพียงพอเหมาะสมตามขอบเขตระดับความเสี่ยงและความจำเป็นสำคัญของการใช้บริการ การเชื่อมต่อ	ลูกค้าควรกำหนดและดำเนินขั้นตอนเกี่ยวกับเครือข่ายการสื่อสารเพื่อป้องกันการเชื่อมต่อเครือข่ายที่ไม่ปลอดภัยดำเนินการหรือติดตั้งมาตรการหรืออุปกรณ์ความปลอดภัยเครือข่ายที่จำเป็น เพื่อปกป้องระบบเครือข่ายและเฝ้าระวังภัยคุกคามและบุกรุกความปลอดภัยเครือข่ายได้อย่างทันท่วงที ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เน็ต Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจว่ามีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า Direct Connect (DC): จัดเตรียมการเชื่อมต่อเครือข่ายแบนด์วิดท์สูงที่มีความเฉพาะตัวและความปลอดภัยสูง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		หรือการเข้าถึงข้อมูลจากบุคคลภายนอก	ผู้ใช้เป็นเจ้าของลิงก์เครือข่ายโดยเฉพาะ ไม่มีความเสี่ยงข้อมูลรั่วไหล นอกจากนี้ ลูกค้ายังสามารถใช้ Cloud Connect Network (CCN) เพื่อให้บรรลุการเชื่อมต่ออินเทอร์เน็ตที่ปลอดภัยระหว่าง Virtual Private Cloud (VPC) บนคลาวด์ และระหว่าง VPC กับศูนย์ข้อมูลในพื้นที่ (IDC) สำหรับข้อกำหนดการแบ่งส่วนเครือข่าย ลูกค้าสามารถใช้บริการ Virtual Private Cloud (VPC) ที่ Tencent Cloud ให้มาเพื่อสร้างพื้นที่เครือข่ายอิสระหลายแห่งสำหรับทรัพยากรแพลตฟอร์มคลาวด์ที่ได้ซื้อไปแล้ว และกำหนดการแบ่งส่วนเครือข่ายและที่อยู่ IP นโยบายการกำหนดเส้นทาง ฯลฯ ตามต้องการได้ด้วยตนเอง เพื่อดำเนินการป้องกันขอบเขตเครือข่าย Tencent Cloud ให้บริการ EdgeOne (EO) แก่ลูกค้า โดยอิงตามโมเดลขอบข่ายโลกของ Tencent Cloud เพื่อมอบบริการป้องกันความปลอดภัยและเร่งความเร็วให้กับลูกค้า มีฟังก์ชัน เช่น การป้องกัน DDoS การป้องกันเว็บอัจฉริยะ การป้องกันการโจมตีประเภทบอท/ครอว์เลอร์ การแก้ไข DNS และสนับสนุนให้ลูกค้าสามารถกำหนดกฎการควบคุมการเข้าถึงแบบกำหนดเองตามความต้องการทางธุรกิจ Cloud Firewall (CFW) ให้การป้องกันขอบเขตเครือข่ายที่แตกต่างกันแก่ลูกค้าเป็นหลัก สนับสนุนการควบคุม ACL ของไฟร์วอลล์อย่างเข้มข้น การปิดกั้น IPS แบบเรียลไทม์ การปะชุนเสมือน และการตรวจจับโค้ดที่เป็นอันตราย ฯลฯ สามารถตอบสนองความต้องการของโซน DMZ ในเครือข่ายแบบดั้งเดิม ปกป้องสินทรัพย์หลักเป็นพิเศษ และบรรลุการควบคุมการแยกอย่างละเอียดระหว่าง VPC Web Application Firewall (WAF) สามารถจัดการกับปัญหาความปลอดภัยของเว็บไซต์และธุรกิจเว็บ เช่น การโจมตีเว็บ การบุกรุก การใช้ประโยชน์จากช่องโหว่ การฝังมัลแวร์ การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต แบ็กดอร์ ครอว์เลอร์ ฯลฯ Anti-DDoS ใช้ทรัพยากรป้องกัน DDoS ที่มีคุณภาพและเพียงพอ ร่วมกับอัลกอริทึมการทำความสะอาดที่พัฒนาอย่างต่อเนื่อง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			อง "การพัฒนาด้วยตนเอง + การระบุอัจฉริยะด้วย AI" เพื่อจัดการกับปัญหาการโจมตี DDoS สำหรับการแยกหลายผู้เช่า (Multi-tenancy Isolation) Tencent Cloud มีกลไกความปลอดภัย เช่น นโยบายการควบคุมการเข้าถึงทรัพยากรในชั้นควบคุมเสมือน (Virtualization Control Layer) นโยบายการแยกระหว่างเครือข่ายส่วนตัวภายในแพลตฟอร์มคลาวด์ การจัดสรรสิทธิ์และการยืนยันตัวตนบนเว็บคอนโซล รหัสเซสชันของอินเทอร์เน็ตโฟล และคีย์การเข้าถึง เพื่อให้มั่นใจว่าผู้ใช้แต่ละคนสามารถเข้าถึงทรัพยากรคอมพิวเตอร์คลาวด์ที่ตนซื้อได้เท่านั้น ซึ่งทำให้เกิดการแยกการเข้าถึงระหว่างผู้เช่าหลายรายได้อย่างมีประสิทธิภาพ ในด้านการจัดการควบคุมความปลอดภัยเครือข่าย Tencent Cloud ได้ปรับใช้สถาปัตยกรรมความปลอดภัยเครือข่ายที่ครบถ้วน โดยใช้กลไกการป้องกันหลายชั้น เช่น ไฟร์วอลล์ ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) การป้องกัน DDoS การแยกทางตรรกะของเครือข่าย และความปลอดภัยของแอปพลิเคชันเว็บ เพื่อตรวจจับกรอง และบล็อกการรับส่งข้อมูลเครือข่ายที่เป็นอันตรายได้ทันท่วงที ปกป้องความปลอดภัยเครือข่ายของ Tencent Cloud ยังติดตั้งระบบตรวจสอบเครือข่ายภายในเพื่อตรวจสอบและแจ้งเตือนอุปกรณ์เครือข่าย เช่น เราเตอร์ ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย นอกจากนี้ Tencent Cloud ใช้มาตรการต่างๆ เช่น การควบคุมสิทธิ์และขั้นตอนการอนุมัติ เพื่อห้ามไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงทรัพยากรเครือข่ายภายใน ซึ่งรวมถึงเครื่องมือวิเคราะห์และตรวจสอบเครือข่าย สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความปลอดภัยในการสื่อสาร โปรดดูเนื้อหาในข้อ "5 การรักษาความมั่นคงปลอดภัยของระบบเครือข่าย สื่อสาร" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ"

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ในคู่มือนี้
12.5	การบริหารจัดการการเปลี่ยนแปลง	(1) กำหนดกระบวนการและแนวทางการจัดการการเปลี่ยนแปลงร่วมกับบุคคลภายนอก เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถประเมินผลกระทบและเตรียมแนวทางรองรับ เช่น เมื่อมีการเปลี่ยนแปลงระบบของผู้ให้บริการ cloud computing และกระทบกับ การให้บริการและดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (2) ให้บุคคลภายนอกแจ้งการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีผลกระทบกับการให้บริการและดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจได้ทราบล่วงหน้าในระยะเวลาที่ตกลงร่วมกัน เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจพิจารณาแนวทางลดผลกระทบต่อการให้บริการลูกค้าของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ	ลูกค้าควรร่วมกับหน่วยงานภายนอกกำหนดขั้นตอนการจัดการการเปลี่ยนแปลง เพื่อให้การเปลี่ยนแปลงของสินทรัพย์ข้อมูลได้รับการประเมิน ทดสอบ ทบทวน และอนุมัติก่อนการดำเนินการ และกำหนดให้หน่วยงานภายนอกแจ้งการเปลี่ยนแปลงใดๆ ที่อาจส่งผลกระทบต่อการทำงานทางธุรกิจของตนภายในระยะเวลาที่ตกลงกัน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานการจัดการสำหรับการเปลี่ยนแปลงผลิตภัณฑ์และการกำหนดค่าที่กำหนดขั้นตอนต่างๆ ในกระบวนการเปลี่ยนแปลงและผู้รับผิดชอบที่เกี่ยวข้องอย่างชัดเจน เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการอนุมัติและทดสอบอย่างเหมาะสมก่อนการดำเนินการ ในเวลาเดียวกัน Tencent Cloud ได้กำหนดขั้นตอนการจัดการสำหรับการเปลี่ยนแปลงฉุกเฉิน โดยการเปลี่ยนแปลงฉุกเฉินต้องได้รับการอนุมัติที่เหมาะสมก่อนจึงจะสามารถดำเนินการได้ การเปลี่ยนแปลงโปรแกรมทุกประเภท รวมถึงการเปลี่ยนแปลงแอปพลิเคชันและไฟล์กำหนดค่าระบบปฏิบัติการ และฐานข้อมูล ต้องได้รับการวิเคราะห์ผลกระทบทางธุรกิจก่อนการเปิดตัว จัดทำแผนย้อนกลับสำหรับการเปลี่ยนแปลง และได้รับการอนุมัติจากผู้รับผิดชอบที่เกี่ยวข้อง ระบบเผยแพร่การเปลี่ยนแปลงของ Tencent Cloud บังคับให้การดำเนินการเปลี่ยนแปลงสามารถดำเนินการได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น และเก็บรักษาบันทึกที่เกี่ยวข้องกับการเปลี่ยนแปลงไว้ พร้อมทั้งตรวจสอบบันทึกเป็นประจำ หลังการเผยแพร่การเปลี่ยนแปลง Tencent Cloud จะตรวจสอบ ตรวจสอบ และบันทึกผลการเปลี่ยนแปลงในสภาพแวดล้อมการผลิต Tencent Cloud จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอการดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน และขอบเขตของการเปลี่ยนแปลง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแวดล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขยาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการเปลี่ยนแปลง โปรดดูเนื้อหาในข้อ "6.8 บริหารจัดการการเปลี่ยนแปลง" ของ "5.3 <u>เอกสารแนบ 2</u> <u>การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ</u> <u>ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ</u> ในคู่มือนี้
12.6	การบริหารจัดการการตั้งค่าระบบ	กรณีบุคคลภายนอกมีหน้าที่เปลี่ยนแปลงการตั้งค่าระบบงาน สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรกำหนดมาตรฐานการตั้งค่าระบบงานให้ปลอดภัยเพียงพอตามมาตรฐานด้านความปลอดภัยเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจเช่น ค่า system configuration ของระบบปฏิบัติการ และการตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย เป็นต้น	ลูกค้าควรให้มั่นใจว่าเมื่อหน่วยงานภายนอกรับผิดชอบการเปลี่ยนแปลงการกำหนดค่าระบบ ลูกค้าควรมีมาตรฐานการกำหนดค่าความปลอดภัยของตนเองและสร้างกระบวนการที่เกี่ยวข้องเพื่อตรวจสอบความเปี่ยงเบนของการกำหนดค่าในระบบจากมาตรฐานความปลอดภัย <u>Cloud Security Center (CSC)</u> ให้ฟังก์ชันการตรวจสอบและประเมินความเสี่ยงการกำหนดค่าผลิตภัณฑ์คลาวด์โดยอัตโนมัติ ช่วยลูกค้าลดความเสี่ยงด้านความปลอดภัยที่เกิดจากข้อผิดพลาดในการกำหนดค่าความปลอดภัยในการใช้ผลิตภัณฑ์คลาวด์ และยกระดับความปลอดภัยโดยรวมบนคลาวด์ ในเวลาเดียวกัน ลูกค้าสามารถใช้ <u>Config</u> เพื่อดำเนินการตรวจสอบและควบคุมทรัพยากรคลาวด์บางส่วนกลาง บันทึกข้อมูลการกำหนดค่าและการเปลี่ยนแปลงการกำหนดค่าของทรัพยากรคลาวด์ต่างๆ ในภูมิภาคต่างๆ ภายใต้บัญชีของลูกค้าอย่างต่อเนื่อง และอิงตามกฎข้อปฏิบัติที่ดีที่สุดและเทมเพลตแพ็คเกจการปฏิบัติตามข้อกำหนดของ Tencent Cloud เพื่อประเมินความสอดคล้องของการกำหนดค่าทรัพยากรคลาวด์ภายใต้บัญชีองค์กรอย่างต่อเนื่องโดยอัตโนมัติ และระบุการกำหนดค่าทรัพยากรที่ไม่สอดคล้อง เพื่อให้บรรลุการตรวจสอบและจัดการทรัพยากรคลาวด์โดยอัตโนมัติ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อให้สอดคล้องกับข้อกำหนดการกำกับดูแลของลูกค้า Tencent Cloud ได้กำหนดมาตรฐานการกำหนดค่าความปลอดภัยเครือข่ายและมาตรฐานเส้นฐานความปลอดภัยขึ้น เพื่อจัดการมาตรฐานการกำหนดค่าความปลอดภัยของอุปกรณ์เครือข่าย ไฟร์วอลล์ ระบบปฏิบัติการของเซิร์ฟเวอร์โฮสต์ ฐานข้อมูล และระบบแอปพลิเคชัน Tencent Cloud ใช้เครื่องมือสแกนเพื่อตรวจจับความเบี่ยงเบนของการกำหนดค่าระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และอิมเมจเสมือน (Virtual Image) จากมาตรฐานอย่างต่อเนื่อง สำหรับความเบี่ยงเบนที่ตรวจพบ Tencent Cloud จะสร้างใบงานความปลอดภัยและส่งไปยังทีมงานผู้รับผิดชอบโดยอัตโนมัติ เพื่อดำเนินการแก้ไขทันทีที่ Tencent Cloud ยังทบทวนนโยบายความปลอดภัยและการตั้งค่าพารามิเตอร์ของอุปกรณ์เครือข่าย เช่น เราเตอร์ ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย เป็นระยะ เพื่อให้มั่นใจในประสิทธิภาพของนโยบายและพารามิเตอร์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการกำหนดค่าระบบ โปรดดูเนื้อหาในข้อ "6.9 บริหารจัดการการตั้งค่าระบบ" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
12.7	การบริหารจัดการ การขีดความสามารถของ ระบบ	(1) มีกระบวนการติดตาม ประเมินประสิทธิภาพและความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศ ของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก อย่างเพียงพอและต่อเนื่อง ตลอดจนรายงานผลการติดตามและประเมินดังกล่าวให้คณะกรรมการ หรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความ พร้อมใช้และความเพียงพอของระบบ	ลูกค้าควรเฝ้าติดตามการใช้ทรัพยากรระบบเทคโนโลยีสารสนเทศที่บริการภายนอกอย่างต่อเนื่อง กำหนดขีดจำกัดประสิทธิภาพและความจุ และดำเนินการที่จำเป็นเพื่อจัดการกับสถานการณ์ที่เกินขีดจำกัดที่กำหนดไว้ล่วงหน้า เพื่อให้บรรลุการตรวจสอบและจัดการประสิทธิภาพของระบบ ลูกค้าสามารถใช้ Tencent Cloud Observability Platform (TCOP) ซึ่งให้บริการตรวจสอบแบบเรียลไทม์ การวิเคราะห์ และการแจ้งเตือนสำหรับผลิตภัณฑ์/ทรัพยากรคลาวด์ รวบรวมและแสดงตัวชี้วัดการตรวจสอบต่างๆ ที่รายงานโดยผลิตภัณฑ์คลาวด์ เช่น เซิร์ฟเวอร์คลาวด์และฐานข้อมูลคลาวด์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง รวมทั้งเพื่อพิจารณาแนวทางลดความเสี่ยงได้ทันการณ์ (2) กำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (threshold และ trigger) ในระดับต่าง ๆ และกำหนดกระบวนการรายงานและแจ้งเตือน ปัญหาหรือเหตุการณ์ผิดปกติที่เกิดจากการให้บริการหรือเชื่อมต่อกับบุคคลภายนอก แนวทางการประสานงานกับหน่วยงานทั้งภายในและภายนอกกรณีเกิดเหตุขัดข้อง ให้เพียงพอเหมาะสมตามขอบเขตระดับความเสี่ยงและ ความมีนัยสำคัญของบริการ เพื่อให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจทราบอย่างทัน การณ์	รวมถึงตัวชี้วัดการตรวจสอบที่กำหนดเองและรายงานโดยลูกค้าผ่านแผนภูมิที่มองเห็นได้ ช่วยให้ลูกค้าติดตามอัตราการใช้ทรัพยากรผลิตภัณฑ์คลาวด์ ประสิทธิภาพของแอปพลิเคชัน และสถานะการทำงานของผลิตภัณฑ์คลาวด์แบบเรียลไทม์ และสนับสนุนการตั้งค่าการแจ้งเตือนตามตัวชี้วัด โดยแจ้งให้ลูกค้าทราบถึงความผิดปกติของธุรกิจอย่างทันท่วงทีผ่านการส่งข้อความและช่องทางอื่นๆ ตามกฎหมายการแจ้งเตือนที่ตั้งไว้ Tencent Cloud ทำการคาดการณ์ความต้องการด้านความจุตามความต้องการในการดำเนินงานทางธุรกิจ และจัดทำแผนการจัดการความจุประจำปี โดยใช้แพลตฟอร์มตรวจสอบความจุภายในเพื่อให้เจ้าหน้าที่จัดการความจุเฝ้าติดตามสถานการณ์การใช้ความจุ และตรวจสอบการใช้งานความจุแบบเรียลไทม์ และระบุแนวโน้มการใช้ความจุ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการความจุโปรดดูเนื้อหาในข้อ "6.1 บริหารจัดการขีดความสามารถของระบบเทคโนโลยีสารสนเทศและระบบสารสนเทศ ของ "5.3 เอกสารแนบ 2 <u>การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ</u> <u>ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ</u> ในคู่มือนี้
12.8	การจัดเก็บข้อมูลบันทึกเหตุการณ์	ดูแลให้มั่นใจว่าบุคคลภายนอกมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ที่ครบถ้วนเพียงพอและปลอดภัย เพื่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้ติดตามตรวจสอบร่องรอยการเข้าถึงและการใช้งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานการทำการธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด	ค่าควรสร้างกลไกการจัดการบันทึกเพื่อให้มั่นใจว่าหน่วยงานภายนอกจะรวบรวม ประมวลผล และวิเคราะห์บันทึกของระบบ และระบุพฤติกรรมที่น่าสงสัยหรือผิดปกติ Tencent Cloud ให้บริการ <u>Cloud Log Service (CLS)</u> เพื่อช่วยเหลือผู้ใช้ในการแก้ไขปัญหาด้านการดำเนินการธุรกิจ การตรวจสอบความปลอดภัย การตรวจสอบบันทึก และการวิเคราะห์บันทึกผ่านบันทึก Tencent Cloud CLS ใช้การออกแบบสถาปัตยกรรมแบบกระจายที่มีความพร้อมใช้งานสูง จัดเก็บข้อมูลบันทึกด้วยการสำรองข้อมูลหลายชุด

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ป้องกันไม่ให้ข้อมูลไม่สามารถใช้งานได้เมื่อบริการไหนเดิ ยขาดข้อง ให้บริการที่มีความพร้อมใช้งานสูง และรับประกันบริการที่เสถียรและน่าเชื่อถือสำหรับข้อมูล บันทึก ด้วย CloudAudit ผู้ใช้สามารถบันทึกบันทึก ตรวจสอบอย่างต่อเนื่อง และเก็บรักษากิจกรรมบัญชีที่เกี่ยวข้องกับการดำเนินการ ในโครงสร้างพื้นฐาน Tencent Cloud ทั้งหมด ลูกค้าสามารถใช้บริการ Elasticsearch Service (ES) เพื่อรวบรวมและส่งบันทึกแบบเรียลไทม์ของเซิร์ฟเวอร์คลา วด์ คอนเทนเนอร์ และผลิตภัณฑ์คลาวด์อื่นๆ หรือข้อมูลธุรกิจที่มีอยู่และเพิ่มขึ้นของธุรกิจ ไปยังคลัสเตอร์ ES ของ Tencent Cloud เพื่อจัดเก็บข้อมูลแบบกระจาย และการสืบค้นและการวิเคราะห์ข้อมูล เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกั บดูแล Tencent Cloud ได้สร้างมาตรฐานและกลไกการรวบรวมและการจัดการบัน ทึก เพื่อควบคุมการบันทึก การดึงข้อมูล การจัดเก็บ การป้องกัน การวิเคราะห์ และการตรวจสอบบันทึกต่างๆ เช่น บันทึกการเข้าสู่ระบบ บันทึกการดำเนินการ บันทึกระบบทั่วไป และบันทึกเหตุการณ์ความปลอดภัยของระบบ เพื่อตรวจจับและป้องกันความผิดปกติและความเสี่ยงของ กิจกรรมระบบ บันทึกทั้งหมดถูกรวมเข้าสู่แพลตฟอร์มการจัดการบันทึก ของ Tencent Cloud เพื่อการจัดการ และมีการใช้มาตรการสำรองข้อมูลและการป้องกันที่เข้มง วดสำหรับข้อมูลบันทึกที่เกี่ยวข้อง เพื่อป้องกันการแก้ไขและการลบโดยไม่ได้รับอนุญาต Tencent Cloud ดำเนินการตรวจสอบบันทึกผ่านเครื่องมือตรวจสอบอัตโนมัติโน มัติด้านความปลอดภัยในการปฏิบัติการและทีมตรวจสอบ ภายใน เพื่อตรวจจับความผิดปกติของระบบหรือการดำเนินการ เพื่อป้องกันความเสี่ยงในการปฏิบัติการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการบันทึกประวัติ โปรดดูเนื้อหาในข้อ "6.4 จัดเก็บข้อมูลบันทึกเหตุการณ์" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสา รสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
12.9	การติดตามดู และระบบและเ ฝ้าระวังภัยคุ คาม		<u>ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ"</u> ในคู่มือนี้
		(1)ดูแลบุคคลภายนอกให้ติดตามดูแ ลระบบและเฝ้าระวังภัยคุกคามอย่างร ดกุมเพียงพอและ ต่อเนื่อง รวมทั้งระบบ/บริการที่มีนัยสำคัญ ควรมีการตรวจจับเหตุการณ์ผิดปกติที่กระทบ ต่อความปลอดภัยทั้งในระดับ system network และ application เพื่อรับมือภัยคุกคามได้ อย่างทันการณ์ (2)จัดให้มีการวิเคราะห์ข้อมูลบันทึก เหตุการณ์ (logging) ของระบบ/บริการที่ใช้หรือเชื่อมต่อ กับ บุคคลภายนอก เพื่อป้องกันและตรวจจับการบุกรุก	ลูกค้าควรสร้างความสามารถในการรับรู้สถานการณ์ความ ปลอดภัยทางไซเบอร์ เพื่อเฝ้าระวังภัยคุกคามที่เกิดขึ้นใหม่ และตรวจจับเหตุการณ์ผิดปกติและภัยคุกคามที่มีผลต่อระ บบสำคัญ เพื่อเพิ่มความมั่นใจในการค้นพบ การป้องกัน และการตอบสนองได้ทันเวลาที่ เพื่อสนับสนุนลูกค้าในการตรวจจับและวิเคราะห์ภัยคุกคาม Tencent Cloud ให้บริการ <u>Threat Intelligence</u> <u>X (TIX)</u> แก่ลูกค้า ซึ่งเป็นแพลตฟอร์มบริการข่าวกรองแบบครบวงจร TIX สามารถให้ความสามารถด้านข่าวกรองสามประเภทหลัก ได้แก่ ข่าวกรองพื้นฐาน ข่าวกรองด้านพื้นผิวการโจมตี และข่าวกรองทางธุรกิจ รองรับฟังก์ชันต่างๆ เช่น การสืบค้นข่าวกรอง การวิเคราะห์และประเมิน IOC การจัดการพื้นผิวการโจมตี สามารถช่วยลูกค้าวิเคราะห์และประเมินเหตุการณ์ความป ลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น และประเมินความเสี่ยงด้านการเปิดเผยสินทรัพย์ขององค์กร อย่างครอบคลุมมากขึ้น สนับสนุนองค์กรในการสร้างระบบป้องกันความปลอดภัยแ บบสามมิติที่มีประสิทธิภาพ ศูนย์ข่าวกรองภัยคุกคามยังสามารถรวมเข้ากับผลิตภัณฑ์ ที่ป้องกันความปลอดภัยที่มีอยู่ของลูกค้าได้ในรูปแบบกา รวมเข้าด้วยกัน เพื่อเชื่อมโยงข้อมูลข่าวกรองจากคลาวด์กับผลิตภัณฑ์ดัง กล่าว เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัยโ ดysseyรวมและการตอบสนองต่อภัยคุกคาม ด้วยการเสริมพลังและการสนับสนุนจากศูนย์ข่าวกรองภัย คุกคาม Tencent Cloud มุ่งมั่นที่จะสร้างระบบความสามารถด้านความปลอดภัยใน การป้องกันเชิงรุกแบบ "ข่าวกรอง- การโจมตีและการป้องกัน-การจัดการ-การวางแผน" โดยบูรณาการเทคโนโลยีต่างๆ เช่น ข่าวกรองภัยคุกคาม ปัญญาประดิษฐ์ ข้อมูลขนาดใหญ่ เพื่อเพิ่มความสามารถและประสิทธิภาพในการตอบสนอง ต่อเหตุการณ์ความปลอดภัย และได้จัดตั้งศูนย์ปฏิบัติการความปลอดภัยที่ทำงาน 24 ชั่วโมงทุกวัน ให้มีความสำคัญกับการตรวจจับภัยคุกคาม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			การสอบสวน และการตอบสนอง เพื่อให้บรรลุความสามารถในการรับรู้มองเห็น และควบคุมสถานการณ์ความปลอดภัย สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบความปลอดภัย โปรดดูเนื้อหาในข้อ "6.5 ติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
12.10	การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ	(1)ดูแลให้บุคคลภายนอกมีการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing) ตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป และสอดคล้องกับนโยบายระเบียบวิธีปฏิบัติของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ (2)สอบทานขอบเขตและผลการทดสอบเจาะระบบ (penetration testing) ของบุคคลภายนอก เพื่อให้มั่นใจว่าการทดสอบดังกล่าวครอบคลุมระบบทั้งหมดที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการหรือเชื่อมต่อกับบุคคลภายนอก และครอบคลุมภัยคุกคามที่สำคัญ	ลูกค้าควรดำเนินการประเมินช่องโหว่และการทดสอบเจาะระบบเป็นประจำ เพื่อระบุช่องโหว่ด้านความปลอดภัยและประเมินความสามารถในการป้องกันความปลอดภัยทางไซเบอร์ของตน ในด้านการทดสอบเจาะระบบ Tencent Cloud ให้บริการ Penetration Testing Service (PTS) แก่ลูกค้า ด้วยการจำลองเทคนิคการโจมตีและเทคนิคการค้นพบช่องโหว่ที่แฮกเกอร์อาจใช้อย่างเต็มรูปแบบ ใช้วิธีการและกลไกที่ควบคุมได้และไม่ทำลายล้างเพื่อทำการตรวจสอบความปลอดภัยของระบบเป้าหมายอย่างลึกซึ้ง ค้นหาจุดอ่อนที่มีอยู่ในเป้าหมายและอุปกรณ์เครือข่ายให้คำแนะนำในการเสริมความแข็งแกร่งด้านความปลอดภัยเพื่อช่วยลูกค้ายกระดับความปลอดภัยของระบบ และสนับสนุนการตรวจสอบหลังการแก้ไขช่องโหว่ ในด้านการสแกนช่องโหว่ ลูกค้าสามารถเลือกใช้ Vulnerability Scanning Service (VSS) เพื่อตรวจสอบสินทรัพย์เครือข่ายขององค์กรและระบุความเสียหายของสินทรัพย์นั้นๆ โดยใช้ประโยชน์จากประสบการณ์ด้านความปลอดภัยและข่าวกรองภัยคุกคามที่สะสมมาหลายปีของ Tencent Cloud VSS ได้สร้างฐานข้อมูลกฎช่องโหว่ที่อุดมสมบูรณ์และครอบคลุม และมีความสามารถในการตรวจจับช่องโหว่ 0Day/1Day/NDay ที่มีอาชีวะและมีประสิทธิภาพสูง สามารถดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของสินทรัพย์ของลูกค้า

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ให้คำแนะนำการแก้ไขที่มีอาชีวะแก่ลูกค้า เพื่อลดความเสี่ยงด้านความปลอดภัย VSS ยังสนับสนุนการทำงานร่วมกับผลิตภัณฑ์คลาวด์ เช่น ความปลอดภัยโฮสต์ไฟร์วอลล์แอปพลิเคชันเว็บ เพื่อให้บรรลุจุดประสงค์จากการตรวจสอบความเสี่ยงไปจนถึง การจัดการความเสี่ยง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ดูแล Tencent Cloud จะสร้างงานสแกนเป็นประจำผ่านระบบสแกนช่องโหว่เพื่อ สแกนช่องโหว่ของสินทรัพย์ในสภาพแวดล้อมคลาวด์ และวิเคราะห์ จัดประเภท และดำเนินการแก้ไขช่องโหว่ที่พบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะดำเนินการทดสอบเจาะระบบขนาดใหญ่แบบเต็มวงจร เป็นประจำ และดำเนินการทดสอบเจาะระบบแบบเจาะจงอย่างยืดหยุ่น ในสถานการณ์ต่างๆ เช่น ก่อนการเปิดตัวผลิตภัณฑ์ใหม่หรือเมื่อมีการเปลี่ยนแปลง ครั้งสำคัญ นอกจากนี้ Tencent Cloud ยังดำเนินการฝึกซ้อมการต่อสู้เสมือนระหว่างทีมแดงและที มน้ำเงินเพื่อจำลองการต้านทานการโจมตีทางเครือข่ายเป็น ประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการช่องโหว่และการ ทดสอบเจาะระบบ โปรดดูเนื้อหาในข้อ "6.6 บริหารจัดการช่องโหว่ & 6.7 ทดสอบเจาะระบบ" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสา รสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
12.11	การสำรองข้อ มูล	กรณีนี้ที่สถาบันการเงินและสถาบันการ เงินเฉพาะกิจใช้บริการหรือเชื่อมต่ กับบุคคลภายนอก ซึ่งมีการ จัดเก็บข้อมูลของสถาบันการเงินแล ะสถาบันการเงินเฉพาะกิจ หรือข้อมูลลูกค้า สถาบันการเงินและ สถาบันการเงินเฉพาะกิจควรกำหนด มาตรฐานวิธีปฏิบัติในการสำรองข ้อมูลให้บุคคลภายนอกปฏิบัติ ให้สอดคล้องกับมาตรฐานของสภา	ลูกค้าควรสร้างกลไกการจัดการการสำรองข้อมูล ทำการสำรองข้อมูลตามความถี่ที่กำหนด และดำเนินการทดสอบการกู้คืนจากการสำรองข้อมูลเป็น ประจำ ภายในปี 2026 Tencent Cloud ได้ติดตั้งศูนย์ข้อมูลสามแห่งภายในประเทศไทย โดยแต่ละแห่งมีระบบไฟฟ้าและเครือข่ายที่ทำงานอิสระต่อ กัน สามารถสนับสนุนให้ลูกค้าเก็บข้อมูล ประมวลผล และสำรองข้อมูลภายในประเทศได้ บริการจัดเก็บข้อมูลและบริการฐานข้อมูลหลายรายการที่

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ธนาคารเงินและสถาบันการเงินเฉพาะ กิจ โดยครอบคลุม	Tencent Cloud มอบให้ฟังก์ชันการสำรองข้อมูล พร้อมตอบสนองความต้องการสำรองข้อมูลทุกรูปแบบของ ลูกค้า ตัวอย่างเช่น: ข้อมูลที่ลูกค้าเก็บไว้ใน Cloud Object Storage (COS) สามารถจัดเก็บข้อมูลในหลายพื้นที่ที่กำหนดพร้อม กันได้ผ่านฟังก์ชันการทำสำเนาข้ามพื้นที่ เพื่อให้แน่ใจว่าแม้ในกรณีที่สูญหายข้อมูลบางส่วนไป โดยไม่ได้คาดหมาย ก็ยังสามารถค้นหาและกู้คืนข้อมูลทั้งหมดได้ผ่านข้อ มูลสำรอง และยังหลีกเลี่ยงความเสี่ยงสูญหายที่อาจเกิดขึ้นเมื่อพื้นที่ เก็บข้อมูลในโซนความพร้อมใช้งานหนึ่งประสบภัยพิ บัติที่ไม่อาจหลีกเลี่ยงได้ ซึ่งช่วยให้บรรลุผลสำรองข้อมูลหลายชุดและการกู้คิ นจากภัยพิบัติข้ามพื้นที่ ฟังก์ชันการสำรองข้อมูลแบบสแนปช็อตของ Cloud Block Storage (CBS) ทำการสำรองข้อมูลโดยการถ่ายสแนปช็อต ณ จุดเวลาใดเวลาหนึ่งของ CBS ป้องกันการสูญหายข้อมูลเนื่องจากการแก้ไขโดยไม่ไ ด้รับอนุญาตและการลบผิดพลาด และรับประกันความสามารถในการย้อนกลับอย่างร วดเร็วเมื่อเกิดความขัดข้องทางธุรกิจ Cloud File Storage (CFS) ให้ฟังก์ชันสแนปช็อตเป็นระยะ เพื่อความสะดวกในการตั้งค่านโยบายงานสำรองข้อ มูลตามความยืดหยุ่นของลูกค้า Cloud Native Database TDSQL-C รองรับการสำรองข้อมูลสองประเภท: การสำรองข้อมูลเชิงตรรกะและการสำรองข้อมูลแบบ สแนปช็อต ด้วยการสำรองข้อมูลที่สมบูรณ์และการสำรองข้อมูล binlog ในช่วงเวลาต่อมา ทำให้สามารถกู้คืนคลัสเตอร์ TDSQL-C MySQL Edition ทั้งหมดหรือตารางฐานข้อมูลเฉพาะไปยังจุดเวลาใด ก็ได้ TencentDB for MySQL รองรับสองวิธีในการสำรองข้อมูลฐานข้อมูล:

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			การสำรองข้อมูลอัตโนมัติและการสำรองข้อมูลด้วยตนเอง และให้ฟังก์ชันการสำรองข้อมูลข้ามพื้นที่เพื่อช่วยลูกค้าเพิ่มความสามารถในการกู้คืนจากภัยพิบัติและเพิ่มความน่าเชื่อถือของข้อมูลไปพร้อมๆ กัน TencentDB for MongoDB ให้กลไกการสำรองข้อมูลอัตโนมัติและการกู้คืนโดยไม่มีสูญเสียข้อมูล รองรับการสำรองข้อมูลแบบหลายโหนด ลูกค้าสามารถเก็บข้อมูลสำรองไว้หลายวันผ่านกลไกการสำรองข้อมูล เพื่อความสะดวกในการกู้คืนข้อมูลในสถานการณ์ภัยพิบัติ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการสำรองข้อมูลโปรดดูเนื้อหาในข้อ "6.3 สำรองข้อมูล" ของ "5.3 เอกสารแนบ 2" การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ในคู่มือนี้
12.12	การบริหารจัดการเหตุการณ์ด้านเทคโนโลยีสารสนเทศ	(1) ระบุหน้าที่และความรับผิดชอบของสถาบันการเงินและสถาบันการเงินเฉพาะกิจและบุคคลภายนอกอย่างชัดเจน ในการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศรวมถึงกำหนดระดับความรุนแรงของเหตุการณ์ผิดปกติดังกล่าว และกำหนดให้แจ้งสถาบันการเงินและสถาบันการเงินเฉพาะกิจทราบเหตุการณ์ผิดปกติที่เกิดขึ้นและเกี่ยวข้องกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างเพียงพอและทันการณ์ (2) หากเหตุการณ์ผิดปกติที่เกิดขึ้นนั้นมีผลกระทบต่อการทำงานของสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างมีนัยสำคัญ	ลูกค้าควรกำหนดบทบาทและความรับผิดชอบของตนเองและของหน่วยงานภายนอกในการจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศให้ชัดเจน และกำหนดให้หน่วยงานภายนอกรายงานเหตุการณ์ที่เกี่ยวข้องอย่างทันห่วงที่และเพียงพอ หากเหตุการณ์ไม่มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานธุรกิจ ลูกค้าควรมีส่วนร่วมในการตัดสินใจจัดการเหตุการณ์นอกจากนี้ ลูกค้ายังควรกำหนดให้หน่วยงานภายนอกจัดตั้งช่องทางสื่อสาร เพื่อให้แน่ใจว่าสามารถรายงานความผิดปกติและประสานการตอบสนองได้อย่างทันห่วงที่ เพื่อสนับสนุนลูกค้าในการตรวจจับและตอบสนองต่ออุบัติเหตอย่างรวดเร็ว Tencent Cloud ให้บริการแพลตฟอร์มการจัดการความปลอดภัยแบบครบวงจร Cloud Security Center (CSC) ผ่านฟังก์ชันต่างๆ เช่น ศูนย์สินทรัพย์ ศูนย์ความเสี่ยง ศูนย์แจ้งเตือน และการจัดการความปลอดภัยขั้นสูง ช่วยลูกค้าบรรลุวงจรการดำเนินงานความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติ	ได้แก่ การตรวจจับภัยคุกคามก่อนเกิดเหตุการณ์ การตอบสนองและจัดการระหว่างเกิดเหตุ และการวิเคราะห์ย้อนหลังหลังเหตุการณ์ เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัย
	(3)กำหนดให้บุคคลภายนอกจัดให้มีช่องทาง ระบบ หรือเครื่องมือเพื่อรองรับกรณีสถาบันการเงินและสถาบันการเงินเฉพาะกิจตรวจพบและต้องการรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศให้บุคคลภายนอกทราบ และเพื่อช่วยให้สถาบันการเงินและสถาบันการเงินเฉพาะกิจติดตามสถานการณ์ และการแก้ไขของบุคคลภายนอกต่อเหตุการณ์ผิดปกติที่เกี่ยวข้องกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจได้อย่างทันการณ์		ในการกำหนดบทบาทและความรับผิดชอบระหว่างลูกค้าและ Tencent Cloud ในกรณีเกิดเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ ได้จัดเตรียมเอกสารกฎหมายออนไลน์ เช่น Terms of Service Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งเนื้อหาประกอบด้วย: การจัดทำสัญญาจ้างทำภายนอก ความสัมพันธ์และหน้าที่ความรับผิดชอบ การแบ่งงานกัน การแจ้งเหตุการณ์ กลไกการระงับข้อพิพาท และประเด็นความคาดหวังอื่นๆ ของคู่สัญญา นอกจากนี้ลูกค้ายังสามารถเจรจาเพื่อเพิ่มข้อกำหนดพิเศษลงในสัญญาแยกต่างหากได้
	(4)กำหนดให้บุคคลภายนอกมีผู้ประสานงานอย่างเป็นทางการ เพื่อประสานงานกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจในการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศได้ อย่างทันการณ์		ในด้านการตรวจจับและตอบสนองต่อเหตุการณ์ Tencent Cloud ได้สร้างขั้นตอนการจัดการเหตุการณ์โดยละเอียด โดยใช้ระบบการดำเนินงานความปลอดภัยภายในเพื่อบันทึกเหตุการณ์ความปลอดภัย สำหรับเหตุการณ์ความปลอดภัยที่ตรวจจับและระบุได้ Tencent Cloud จะวิเคราะห์และจำแนกระดับเหตุการณ์โดยพิจารณาจากปัจจัยต่างๆ เช่น ลักษณะของเหตุการณ์ ระดับความอ่อนไหวของข้อมูล และขอบเขตของผลกระทบ และจะแจ้งให้ผู้รับผิดชอบที่เกี่ยวข้องทราบทันทีเพื่อดำเนินการจัดการเหตุการณ์ ทีมงานความปลอดภัยของ Tencent Cloud ใช้ระบบการดำเนินงานความปลอดภัยแบบ 24 ชั่วโมงทุกวัน โดยมุ่งเน้นไปที่สถานการณ์หลัก เช่น การเฝ้าระวังช่องโหว่ การติดตามแหล่งที่มาของการบุกรุก และการปิดกั้นการโจมตี ตอบสนองต่อการแจ้งเตือนความปลอดภัยแบบเรียลไทม์และจัดทำแผนการติดตามแหล่งที่มาของการโจมตีและการจัดการเหตุการณ์ฉุกเฉินอย่างรวดเร็ว เพื่อยับยั้งการแพร่กระจายของเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพ
			สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			บตอลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้เหลือน้อยที่สุด ในด้านการที่ลูกค้าแจ้งปัญหาหรือติดต่อ Tencent Cloud คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการในงาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับ ระบบในงานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับในงานของลูกค้าผ่านกลไกการตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมและจัดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้าได้รับการตอบสนองและจัดการอย่างทันทั่วถึง นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้าได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเวลา ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับการสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการเหตุการณ์ด้านเทคโนโลยีสารสนเทศ โปรดดูเนื้อหาในข้อ "8 การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา"

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
12.13	การบริหารความต่อเนื่องทางธุรกิจ	(1) มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan) และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (disaster recovery plan) ที่ครอบคลุมถึงการให้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เพื่อให้มีแนวทางรองรับต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อสถาบันการเงินและสถาบันการเงินเฉพาะกิจอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการและดำเนินธุรกิจได้อย่างต่อเนื่อง (2) แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศควรคำนึงถึงปัจจัยสำคัญหรือความเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบต่อการทำงานของบริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ผลกระทบที่มีต่อการให้บริการและดำเนินธุรกิจของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ และการติดต่อสื่อสารระหว่างบุคคลภายนอกกับสถาบันการเงินและสถาบันการเงินเฉพาะกิจ รวมถึงการรายงานปัญหา หรือเหตุการณ์ผิดปกติให้คณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างทันการได้ตามความสำคัญและระดับความรุนแรงหรือผลกระทบของเหตุ	ลูกค้าควรสร้างกลไกการจัดการความต่อเนื่องของธุรกิจ จัดทำแผนความต่อเนื่องของธุรกิจที่ครอบคลุมบริการภายนอก ดำเนินการวิเคราะห์ผลกระทบทางธุรกิจ กำหนดเป้าหมายเวลาในการกู้คืน (RTO) และเป้าหมายจุดข้อมูลในการกู้คืน (RPO) ของแต่ละธุรกิจให้ชัดเจน จัดทำแผนฉุกเฉินเพื่อความต่อเนื่องของธุรกิจ และสื่อสารไปยังผู้ที่เกี่ยวข้อง นอกจากนี้ ลูกค้ายังควรตรวจสอบและทดสอบการดำเนินการตามแผนฉุกเฉินอย่างน้อยปีละครั้ง เพื่อให้มั่นใจว่าลูกค้าสามารถตอบสนองและกู้คืนฟังก์ชันสำคัญได้อย่างรวดเร็วหลังเกิดเหตุการณ์ภัยพิบัติ ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud ให้มา เช่น บริการคอมพิวเตอร์ บริการเครือข่าย บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ บริการความปลอดภัย ส่วนมีคุณลักษณะความพร้อมใช้งานสูง และมีแผนการกู้คืนจากภัยพิบัติที่สอดคล้องกัน เช่น: Cloud Load Balancer (CLB) ให้บริการกระจายปริมาณข้อมูลระดับ 4 และ 7 ที่ปลอดภัยและรวดเร็ว โดยขยายความสามารถในการให้บริการภายนอกของระบบแอปพลิเคชันผ่านการกระจายปริมาณข้อมูล และจัดจุดล้มเหลวเพียงจุดเดียว CLB ใช้การปรับใช้แบบคลัสเตอร์ และจะลบอินสแตนซ์ที่ขัดข้องออกทันทีเพื่อให้บรรลุความพร้อมใช้งานสูง Cloud Virtual Machine (CVM) มีคุณลักษณะของความพร้อมใช้งานสูงของบริการและความน่าเชื่อถือสูงของข้อมูล Cloud Block Storage ที่ใช้กับ CVM ให้กลยุทธ์การจัดเก็บข้อมูลสำรองสามชุด ซึ่งรับประกันความสามารถในการย้ายและกู้คืนข้อมูลได้อย่างรวดเร็วเมื่อสำเนาใดสำเนาหนึ่งขัดข้อง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		การณ	
		(3)ประเมินและทดสอบการปฏิบัติตามแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศเพื่อให้สามารถปฏิบัติงานได้จริง รวมถึงสอบทานแผนของบุคคลภายนอกเพื่อพิจารณาความสอดคล้องกับแผนของสถาบันการเงินและสถาบันการเงิน เฉพาะกิจ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : maximum tolerable period of disruption (MTPD), recovery time objective (RTO) และ recovery point objective (RPO) เป็นต้น	• <u>Cloud Object Storage (COS)</u> ให้การจัดเก็บข้อมูลสำรองหลายชุดผ่านหลายสถาปัตยกรรมและหลายอุปกรณ์ จัดเตรียมฟังก์ชันการกู้คืนจากภัยพิบัติข้ามพื้นที่และการแยกทรัพยากรสำหรับข้อมูลลูกค้า และให้บรรลุความคงทนของข้อมูล • <u>TencentDB for MySQL</u> รองรับความน่าเชื่อถือสูงของข้อมูลและความพร้อมใช้งานสูงของบริการ และมีกลไกการสำรองข้อมูลอัตโนมัติและการกู้คืนโดยไม่สูญเสียข้อมูลที่สมบูรณ์ • <u>Tencent Kubernetes Engine (TKE)</u> ใช้สถาปัตยกรรมบริการแบบกระจาย รับประกันการกู้คืนโดยอัตโนมัติจากการขัดข้องของบริการและการย้ายถิ่นฐานอย่างรวดเร็ว ผสานกับที่เก็บข้อมูลแบบกระจายสำหรับบริการแบบมีสถานะ (Stateful) เพื่อให้บรรลุความปลอดภัยและความพร้อมใช้งานสูงของบริการและข้อมูล
		(4)หากสถาบันการเงินและสถาบันการเงินเฉพาะกิจสามารถเข้าร่วมทดสอบกับบุคคลภายนอกได้ สถาบันการเงินและสถาบันการเงินเฉพาะกิจควรเข้าร่วมทดสอบการปฏิบัติตามแผนรองรับ การดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศกับบุคคลภายนอก เพื่อประเมินความพร้อมของบุคคลภายนอกในการกู้คืนระบบงานตามกรอบ MTPD, RTO และ RPO ที่กำหนดไว้	นอกจากนี้ ลูกค้าสามารถใช้บริการ <u>Tencent Cloud Smart Advisor (TSA)</u> เพื่อช่วยในการวางแผนและดำเนินการทดสอบความพร้อมของธุรกิจ Cloud Advisor สามารถจัดเตรียมสถานการณ์การฉีดความล้มเหลว (Fault Injection) ทุกระดับตั้งแต่ IaaS ถึง PaaS รวมถึงเทมเพลตประสบการณ์การฝึกซ้อมจากหลายอุตสาหกรรม ซึ่งครอบคลุมสถานการณ์แอปพลิเคชันทั่วไปหลายด้าน เช่น การกู้คืนจากภัยพิบัติข้าม Availability Zone เพื่อช่วยลูกค้าใช้โซลูชันที่พัฒนาอย่างเต็มที่อย่างรวดเร็วและมีประสิทธิภาพตามความต้องการทางธุรกิจของตนเอง และเพิ่มความพร้อมใช้งานของระบบ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud มีการแยกจากกันโดยสมบูรณ์ระหว่างภูมิภาคต่างๆ เพื่อรับประกันความเสถียรและความทนทานต่อข้อผิดพลาดสูงสุดระหว่างภูมิภาคต่างๆ เพื่อให้มั่นใจในความพร้อมใช้งานสูงของข้อมูล Tencent Cloud แบ่งแต่ละภูมิภาคออกเป็นหลาย Availability Zone ที่แยกจากกัน การออกแบบหลาย Availability
		(5)ทีมบริหารจัดการในสภาวะวิกฤติ (crisis management team) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจควรได้รับทราบถึงรายละเอียดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศของบุคคลภายนอก เพื่อเตรียมความพร้อมในการบริหารจัดการในส่วนที่เกี่ยวข้อง	

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		(6)รวบรวมปัญหาที่พบระหว่างการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและปรับปรุงแก้ไขร่วมกับบุคคลภายนอก	Zone ของ Tencent Cloud สามารถลดผลกระทบจากความล้มเหลวของจุดเดียวได้อย่างมีประสิทธิภาพ และรับประกันว่าความล้มเหลวระหว่าง Availability Zone จะถูกแยกจากกัน ซึ่งจะช่วยรับประกันความต่อเนื่องของธุรกิจของลูกค้า เพื่อให้มั่นใจในความพร้อมใช้งานอย่างต่อเนื่องของธุรกิจลูกค้า Tencent Cloud ได้ออกแบบและนำกรอบการจัดการความต่อเนื่องของธุรกิจที่เหมาะสมกับสภาพแวดล้อมคอมพิวเตอร์คลาวด์ของตนเองไปใช้ และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจ Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภัณฑ์และบริการคลาวด์ กำหนด RTO และ RPO ของแต่ละธุรกิจให้ชัดเจน และจัดทำกลยุทธ์การตอบสนองและแผนความต่อเนื่องของธุรกิจที่แตกต่างกันตามผลการวิเคราะห์ผลกระทบทางธุรกิจ รวมถึงจัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดยละเอียดสำหรับผลิตภัณฑ์คลาวด์ Tencent Cloud จะทำการทดสอบฝึกซ้อมความต่อเนื่องของธุรกิจสำหรับผลิตภัณฑ์คลาวด์เป็นประจำตามแผนความต่อเนื่องของธุรกิจ เพื่อให้มั่นใจในความสามารถในการปฏิบัติได้จริงของแผนแผนฉุกเฉิน ฯลฯ หากลูกค้าประเมินว่าการฝึกซ้อมการกู้คืนจากภัยพิบัติจำเป็นต้องได้รับการมีส่วนร่วมและความร่วมมือจากฝ่าย Tencent Cloud Tencent Cloud จะตอบสนองอย่างแข็งขันและให้ความร่วมมืออย่างเต็มที่ เราจะกำหนดสถานการณ์และขอบเขตการฝึกซ้อมให้ชัดเจนตามความต้องการเฉพาะของลูกค้า ร่วมจัดทำแผนการฝึกซ้อมและแผนการดำเนินการโดยละเอียด ให้การสนับสนุนทางเทคนิคและการประสานทรัพยากรที่จำเป็นระหว่างกระบวนการฝึกซ้อม และช่วยลูกค้าเพิ่มประสิทธิภาพกลยุทธ์และขั้นตอนการกู้คืนจากภัยพิบัติอย่างต่อเนื่อง เพื่อร่วมกันยกระดับความสามารถในการต่อเนื่องของธุรกิจและการกู้คืนจากภัยพิบัติ

5.7.3 การใช้บริการ public cloud computing กับระบบงานสำคัญ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
2	กำหนดปัจจัยในการคัดเลือกบุคคลภายนอกก่อนใช้บริการ	กำหนดปัจจัยในการคัดเลือกบุคคลภายนอกก่อนใช้บริการ โดยอย่างน้อยควรครอบคลุมปัจจัยดังนี้ - ปัจจัยด้านความเสี่ยงของประเทศที่บุคคลภายนอกที่จัดเก็บหรือประมวลผลข้อมูลบนระบบ cloud computing - ปัจจัยด้านการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง - ปัจจัยด้านความยืดหยุ่นในการเปลี่ยนแปลงระบบงานไปยังบุคคลภายนอกรายอื่นหรือการเชื่อมโยง กับระบบอื่นได้	หากลูกค้ามอบหมายระบบที่มีความสำคัญสูง (เช่น ระบบธนาคารหลัก) ให้กับผู้ให้บริการภายนอกดำเนินการผ่านบริการคลาวด์สาธารณะ เกณฑ์การเลือกผู้ให้บริการภายนอกควรรวมถึงความเสี่ยงของประเทศที่ตั้งอยู่ ความเสี่ยงจากความเข้มข้น (concentration risk) และความเสี่ยงด้านการทำงานร่วมกันได้ (interoperability risk) Tencent Cloud ได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบอย่างละเอียดของลูกค้าอย่างเข้มข้น ต่อไปนี้เป็นภาพรวมของแต่ละด้านของเกณฑ์การคัดเลือกที่ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ได้กำหนดไว้สำหรับลูกค้าเมื่อใช้บริการคลาวด์สาธารณะสำหรับระบบที่สำคัญ: ปัจจัยด้านความเสี่ยงของประเทศที่บุคคลภายนอกที่จัดเก็บหรือประมวลผลข้อมูลบนระบบ cloud computing: โครงสร้างพื้นฐานของ Tencent Cloud ครอบคลุมหลายพื้นที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) โดยแต่ละภูมิภาคเป็นพื้นที่ทางภูมิศาสตร์ที่แยกอิสระ และแต่ละโซนความพร้อมใช้งานเป็นโดเมนการบำรุงรักษาและรับมือเหตุขัดข้องที่แยกจากกัน โซนความพร้อมใช้งานแต่ละแห่งถูกแยกทางกายภาพ ลูกค้าสามารถวางระบบและจัดเก็บข้อมูลบนภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระตามความต้องการในการขยายธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อรับประกันความต้องการด้านการรับมือเหตุขัดข้องของธุรกิจ ภายในปี 2026 Tencent Cloud ได้ดำเนินการติดตั้งศูนย์ข้อมูลสามแห่งในประเทศไทย โดยศูนย์ข้อมูลแต่ละแห่งมีการจัดการด้านไฟฟ้าและเครือข่ายที่เป็นอิสระต่อกัน เพื่อรองรับการจัดเก็บประมวลผล และสำรองข้อมูลของลูกค้าภายในประเทศได้อย่างมีประสิทธิภาพ

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ปัจจัยด้านการพึ่งพาบุคคลภายนอกภายใต้ รายหนึ่ง: เพื่อให้มั่นใจว่าลูกค้าสามารถตอบสนองและกู้คืนฟังก์ชัน สำคัญได้อย่างรวดเร็วหลังเกิดเหตุการณ์ภัยพิบัติ ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud ให้มา เช่น บริการคอมพิวเตอร์ บริการเครือข่าย บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ บริการความปลอดภัย ล้วนมีคุณสมบัติความพร้อมใช้งานสูง และมีแผนการกู้คืนจากภัยพิบัติที่สอดคล้องกัน ในเวลาเดียวกัน Tencent Cloud ได้สร้างหรือเข้าศูนย์ข้อมูลในหลายพื้นที่ทั่วโลกตามมา มาตรฐานสากลที่เกี่ยวข้องและข้อกำหนดความปลอดภัยใน ห้องเก็บ เพื่อมอบตัวเลือกภูมิภาคและโซนความพร้อมใช้งานหล ายแห่งให้แก่ลูกค้า เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติ และระดับการบริการของธุรกิจ Tencent Cloud ได้รับการรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจ และได้สร้างระบบการจัดการความต่อเนื่องของธุรกิจที่ค ครอบคลุมภายในองค์กร ดำเนินการฝึกซ้อมและการทดสอบการกู้คืนจากภัยพิบ ติเป็นประจำ เป็นต้น เพื่อให้มั่นใจในความสามารถในการกู้คืนจากภัยพิบัติ ความเร็วในการตอบสนอง และความสามารถในการกู้คืนของระบบและธุรกิจ ปัจจัยด้านความยืดหยุ่นในการเปลี่ยนแปลง ระบบงานไปยังบุคคลภายนอกอื่นหรือ การเชื่อมโยง กับระบบอื่นได้: หากลูกค้าจำเป็นต้องยกเลิกข้อตกลงตามสัญญาเนื่อง จากมีการเปลี่ยนแปลงธุรกิจหรือการวางแผนเทคโนโลยี สารสนเทศในอนาคต ลูกค้าสามารถเลือกทำการสำรองข้อมูลและย้ายข้อมูลแ ละสภาพแวดล้อมการผลิตบนคลาวด์ได้ตลอดเวลา ผลิตภัณฑ์คลาวด์ที่ ตามข้อตกลงการให้บริการระหว่าง Tencent Cloud กับลูกค้า หากบริการคลาวด์หมดอายุหรือสิ้นสุดลง สำหรับข้อมูลที่ลูกค้าเก็บไว้ในเซิร์ฟเวอร์คลาวด์เนื่องจา กการใช้บริการ Tencent Cloud ลูกค้าจำเป็นต้องทำการย้ายข้อมูลให้เสร็จสิ้นก่อนช่วง

ลำดับ ที่	โดเมนการค วาคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เวลาเก็บข้อมูลสิ้นสุดลง Tencent Cloud ให้มารองรับให้ลูกค้าใช้รูปแบบมาตรฐานทั่วไปเพื่อสำรองและย้ายข้อมูลของลูกค้า และลูกค้าสามารถใช้วิธีการส่งและโปรโตคอลการส่งเดียวกันกับขั้นตอนการย้ายขึ้นคลาวด์ หรือใช้บริการเครือข่าย เช่น Direct Connect (DC) VPN Connection เพื่อให้มั่นใจว่าข้อมูลของลูกค้าในขั้นตอนการย้ายออกจากคลาวด์มีความปลอดภัยและเชื่อถือได้ เมื่อบริการคลาวด์สิ้นสุดลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยจะลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรองอย่างสิ้นเชิงหลังจากช่วงเวลาเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้
3	ชี้แจงตำแหน่งก ารประมวลผลแ ละจัดเก็บข้อมูล	กำหนดให้บุคคลภายนอกกระบุสถานที่ในการประมวลผล จัดเก็บข้อมูล หรือดำเนินการอื่นใดที่เกี่ยวข้องกับข้อมูลของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ	หากลูกค้ามอบหมายระบบที่มีความสำคัญสูง (เช่น ระบบธนาคารหลัก) ให้กับผู้ให้บริการภายนอกดำเนินการผ่านบริการคลาวด์สาธารณะ ลูกค้าควรกำหนดให้ผู้ให้บริการภายนอกชี้แจงตำแหน่งทางภูมิศาสตร์ที่เฉพาะเจาะจงสำหรับการประมวลผล การจัดเก็บ หรือการประมวลผลข้อมูลลูกค้าของตน โครงสร้างพื้นฐานของ Tencent Cloud ครอบคลุมหลายพื้นที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) โดยแต่ละภูมิภาคเป็นพื้นที่ทางภูมิศาสตร์ที่แยกอิสระ และแต่ละโซนความพร้อมใช้งานเป็นโดเมนการบำรุงรักษาและรับมือเหตุขัดข้องที่แยกจากกัน โซนความพร้อมใช้งานแต่ละแห่งถูกแยกทางกายภาพ ลูกค้าสามารถวางระบบและจัดเก็บข้อมูลบนภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระตามความต้องการในการขยายธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อรับประกันความต้องการด้านการรับมือเหตุขัดข้องของธุรกิจ ภายในปี 2026 Tencent Cloud ได้ดำเนินการติดตั้งศูนย์ข้อมูลสามแห่งในประเทศไทย โดยศูนย์ข้อมูลแต่ละแห่งมีการจัดการด้านไฟฟ้าและเครือข่ายที่เป็นอิสระต่อกัน เพื่อรองรับการจัดเก็บ ประมวลผล และสำรองข้อมูลของลูกค้าภายในประเทศได้อย่างมีประสิทธิภาพ

ลำดับ ที่	โดเมนการค วาคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สิทธิภาพ Tencent Cloud ดำเนินการตามหลักการเปิดเผยและโปร่งใส หากลูกค้าจำเป็นต้องทราบข้อมูลเกี่ยวกับตำแหน่งการจัดเก็บข้อมูล เช่น ตำแหน่งศูนย์ข้อมูลที่จัดเก็บข้อมูล สถานการณ์การสำรองข้อมูลแบบเย็น (cold backup) และตำแหน่งการจัดเก็บข้อมูลที่สำรองไว้แบบเย็น Tencent Cloud จะจัดเตรียมข้อมูลให้ลูกค้าทันเวลาผ่านช่องทางที่เหมาะสม Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด Tencent Cloud ได้จัดเตรียมเอกสารกฎหมายออนไลน์ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดข้อกำหนดเกี่ยวกับการปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา รวมถึงความรับผิดชอบในการรักษาความลับไว้อย่างชัดเจน
4	ข้อกำหนดการ สำรองข้อมูลสำ หรับบริการคลา วด์นอกประเทศ	กรณีใช้บริการ public cloud computing จากบุคคลภายนอกในต่างประเทศ สถาบันการเงินและ สถาบันการเงินเฉพาะกิจ ควรจัดให้มีกระบวนการสำรองข้อมูล พร้อมทั้งข้อมูลสำรองไว้ในประเทศหรือใน ประเทศอื่นที่มีใช้ประเทศผู้ให้บริการ รวมทั้งสอบถามข้อมูลดังกล่าว อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าข้อมูลมีความพร้อมใช้ และสามารถนำมาใช้ งานได้	ลูกค้าควรสร้างกลไกการจัดการการสำรองข้อมูล ทำการสำรองข้อมูลสำหรับข้อมูลลับและข้อมูลที่ละเอียดอ่อน และเข้ารหัสและปกป้องทางกายภาพสำหรับสื่อจัดเก็บข้อมูลสำรอง และดำเนินการทดสอบการกู้คืนจากการสำรองข้อมูลเป็นประจำ ภายในปี 2026 Tencent Cloud ได้ติดตั้งศูนย์ข้อมูลสามแห่งในประเทศไทย มอบบริการคอมพิวเตอร์คลาวด์หลากหลายประเภท รวมถึงเซิร์ฟเวอร์คลาวด์ ฐานข้อมูลคลาวด์ และ CDN ลูกค้าสามารถเลือกเก็บและประมวลผลข้อมูลของตนในพื้นที่ประเทศไทยได้ ในด้านการจัดการการสำรองข้อมูล บริการจัดเก็บข้อมูลและบริการฐานข้อมูลหลายรายการที่ Tencent Cloud ให้มีส่วนมีฟังก์ชันการสำรองข้อมูล เพื่อตอบสนองความต้องการสำรองข้อมูลทุกประเภท

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ongลูกค้า เช่น Cloud Object Storage (COS) Cloud Block Storage (CBS) Cloud File Storage (CFS) Cloud Native Database TDSQL-C TencentDB for MySQL และ TencentDB for MongoDB เป็นต้น ในด้านการป้องกันการสำรองข้อมูล ผลิตภัณฑ์คลาวด์หลายรายการ เช่น Cloud Native Database TDSQL-C และ Cloud Object Storage (COS) รองรับฟังก์ชันการเข้ารหัสข้อมูลและการควบคุมการเข้า ถึง ซึ่งสามารถรับประกันความเป็นความลับและความสมบูรณ์ ของข้อมูลและข้อมูลสำรองที่เกี่ยวข้องในระหว่างกระ บวนการจัดเก็บได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการสำรองข้อมูล โปรดดูเนื้อหาในข้อ "6.3 สำรองข้อมูล" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีส ารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
5	การเข้ารหัสข้อ มูลที่สำคัญ	จัดให้มีการเข้ารหัสข้อมูลสำคัญตัว ยมาตรฐานสากลทั้งข้อมูลที่อยู่ในส ถานะ data-in-transit และ data-at-rest เมื่อจัดเก็บและประมวลผลบนระบบ public cloud computing ของบุคคลภายนอก	ลูกค้าใช้มาตรฐานสากลในการเข้ารหัสข้อมูลที่จัดเก็บ และประมวลผลบนระบบคลาวด์คอมพิวเตอร์สาธารณะภา ยนอก เพื่อปกป้องความเป็นความลับและความสมบูรณ์ของข้อ มูล เพื่อให้แน่ใจในความเป็นความลับและความสมบูรณ์ของ ข้อมูลลูกค้า ในด้านการป้องกันการจัดเก็บข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการ ของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสานรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล Key Management Service (KMS) ใช้โมดูลความปลอดภัยฮาร์ดแวร์ (HSM) ที่ได้รับการรับรอง FIPS-140-2 ในการสร้างและปกป้องคีย์

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และสามารถสนับสนุนการจัดการวงจรชีวิตเต็มรูปแบบของคีย์การเข้ารหัสของลูกค้าเพื่อลดความเสี่ยงที่คีย์อาจถูกเจาะหรือนำไปใช้ในทางที่ผิด KMS รองรับการหมุนเวียนคีย์และใช้วิธีการลบคีย์ที่หมดอายุ ถูกยกเลิกหรือรั่วไหลออกไปอย่างปลอดภัยและเชื่อถือได้คีย์ที่ถูกลบไปแล้วไม่สามารถกู้คืนได้และข้อมูลที่เข้ารหัสภายใต้คีย์นั้นจะไม่สามารถถอดรหัสได้เช่นกัน นอกจากนี้ Tencent Cloud ใช้เทคโนโลยีการจัดเก็บข้อมูลสำรองหลายชุดและการเข้ารหัสลับล้างข้อผิดพลาดเมื่อจัดเก็บข้อมูลและดำเนินการมาตรการกู้คืนที่จำเป็นเมื่อตรวจพบข้อผิดพลาดด้านความสมบูรณ์ซึ่งช่วยเพิ่มขีดความสามารถในการทนต่อข้อผิดพลาดของข้อมูลอย่างมาก ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มามีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า นอกจากนี้ ลูกค้ายังสามารถใช้บริการ Tencent Cloud ต่อไปเพื่อให้บรรลุการถ่ายโอนข้อมูลที่ปลอดภัยในสถานการณ์ต่างๆ: Direct Connect (DC): จัดเตรียมการเชื่อมต่อเครือข่ายแบนด์วิดท์สูงที่มีความเฉพาะตัวและความปลอดภัยสูง ผู้ใช้เป็นเจ้าของลิงก์เครือข่ายโดยเฉพาะ ไม่มีความเสี่ยงข้อมูลรั่วไหล VPN Connection: อิงตามเทคโนโลยีอุโมงค์เครือข่าย เพื่อให้บรรลุการถ่ายโอนข้อมูลที่ปลอดภัยระหว่างศูนย์ข้อมูลในพื้นที่และทรัพยากรบน Tencent Cloud อุโมงค์ VPN ใช้ IKE (โปรโตคอลแลกเปลี่ยนคีย์ลับ) และ IPsec เพื่อเข้ารหัสข้อมูลที่ถ่ายโอน สร้างอุโมงค์ข้อมูลที่ปลอดภัยและน่าเชื่อถือบนอี

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			นเทอร์เน็ต เพื่อปกป้องความปลอดภัยของข้อมูลระหว่างกา รถ่ายโอน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเข้ารหัสข้อมูลและการ ปกป้องข้อมูล โปรดดูเนื้อหาในข้อ "2 การรักษาความมั่นคงปลอดภัยของข้อมูล" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีส ารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
6	การจัดการการ กำหนดค่าความ ปลอดภัย	จัดให้มีกระบวนการตั้งค่าการรักษา ความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศโดยอ้างอิงแนวปฏิบัติที่ดี ของบุคคลภายนอก หรือมาตรฐานสากล รวมทั้งสอบทานการตั้งค่าดังกล่าว อย่างสม่ำเสมอ	ลูกค้าควรสร้างมาตรฐานการกำหนดค่าความปลอดภัย โดยกำหนดค่าตามแนวปฏิบัติที่ดีที่สุดของผู้ให้บริการ ภายนอกหรือมาตรฐานสากล และสร้างกระบวนการที่เกี่ยวข้องเพื่อตรวจสอบความเป็ ยงเบนของการกำหนดค่าในระบบจากมาตรฐานความป ลอดภัย Cloud Security Center (CSC) ให้ฟังก์ชันการตรวจสอบและประเมินความเสี่ยงการกำ หนดค่าผลิตภัณฑ์คลาวด์โดยอัตโนมัติ ช่วยลูกค้าลดความเสี่ยงด้านความปลอดภัยที่เกิดจาก ข้อผิดพลาดในการกำหนดค่าความปลอดภัยในการใช้ ผลิตภัณฑ์คลาวด์ และยกระดับความปลอดภัยโดยรวมบนคลาวด์ ในเวลาเดียวกัน ลูกค้าสามารถใช้ Config เพื่อดำเนินการตรวจสอบและควบคุมทรัพยากรคลาวด์ จากส่วนกลาง บันทึกข้อมูลการกำหนดค่าและการเปลี่ยนแปลงการกำ หนดค่าของทรัพยากรคลาวด์ต่างๆ ในภูมิภาคต่างๆ ภายใต้บัญชีของลูกค้าอย่างต่อเนื่อง และอิงตามกฎข้อปฏิบัติที่ดีที่สุดและเทมเพลตแพ็คเกจ การปฏิบัติตามข้อกำหนดของ Tencent Cloud เพื่อประเมินความสอดคล้องของการกำหนดค่าทรัพยากร คลาวด์ภายใต้บัญชีองค์กรอย่างต่อเนื่องโดยอัตโนมัติ และระบุการกำหนดค่าทรัพยากรที่ไม่สอดคล้อง เพื่อให้บรรลุการตรวจสอบและจัดการทรัพยากรคลาวด์ โดยอัตโนมัติ เพื่อให้สอดคล้องกับข้อกำหนดการกำกับดูแลของลูกค้า า Tencent Cloud ได้กำหนดมาตรฐานการกำหนดค่าความปลอดภัยเสร็จ

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			อภัยและมาตรฐานเส้นฐานความปลอดภัยขึ้น เพื่อจัดการมาตรฐานการกำหนดค่าความปลอดภัยของ อุปกรณ์เครือข่าย ไฟร์วอลล์ ระบบปฏิบัติการของเซิร์ฟเวอร์โฮสต์ ฐานข้อมูล และระบบแอปพลิเคชัน Tencent Cloud ใช้เครื่องมือสแกนเพื่อตรวจจับความเบี่ยงเบนของการ กำหนดค่าระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และอิมเมจเสมือน (Virtual Image) จากมาตรฐานอย่างต่อเนื่อง สำหรับความเบี่ยงเบนที่ตรวจพบ Tencent Cloud จะสร้างใบงานความปลอดภัยและส่งไปยังทีมงานผู้รับผิดชอบ โดยอัตโนมัติ เพื่อดำเนินการแก้ไขทันทีที่ Tencent Cloud ยังทบทวนนโยบายความปลอดภัยและการตั้งค่าพารามิ เตอร์ของอุปกรณ์เครือข่าย เช่น เราเตอร์ ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย เป็นระยะ เพื่อให้มั่นใจในประสิทธิภาพของนโยบายและพารามิเตอร์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการกำหนดค าระบบ โปรดดูเนื้อหาในข้อ "6.9 บริหารจัดการการตั้งค่าระบบ" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยี สารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
7	การตรวจสอบ เหตุการณ์ความ ปลอดภัยและภัย คุกคาม	มีกระบวนการติดตามเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและ ภัยคุกคามทางไซเบอร์ที่เกิดกับระบบ ที่สถาบันการเงินและสถาบันการเงินเฉพาะกิจใช้บริการ cloud computing อย่างสม่ำเสมอ และมีการกำหนดแนวทางป้องกันภัย คุกคามดังกล่าว เพื่อลดความเสี่ยงที่ อาจเกิดขึ้นก่อนที่บุคคลภายนอก จะสามารถแก้ไขปัญหหรือดำเนินการ patch แล้วเสร็จ	ลูกค้าควรตรวจสอบเหตุการณ์ความผิดปกติด้านความ ปลอดภัยและภัยคุกคามทางเครือข่ายในสภาพแวดล้อม คลาวด์ เพื่อให้แน่ใจว่าเหตุการณ์ความปลอดภัยในสภาพแวดล้อม คลาวด์สามารถถูกตรวจจับและตอบสนองได้ทันท่วง ที่ เพื่อสนับสนุนลูกค้าในการตรวจจับและวิเคราะห์ภัยคุ คาม Tencent Cloud ให้บริการ Threat Intelligence X (TIX) แก่ลูกค้า ซึ่งเป็นแพลตฟอร์มบริการข่าวกรองแบบครบวงจร TIX สามารถให้ความสามารถด้านข่าวกรองสามประเภทหลัก ได้แก่ ข่าวกรองพื้นฐาน ข่าวกรองด้านพื้นผิวการโจมตี และข่าวกรองทางธุรกิจ รองรับฟังก์ชันต่างๆ เช่น การสืบค้นข่าวกรอง การวิเคราะห์และประเมิน IOC การจัดการพื้นผิวการโจมตี

ลำดับ ที่	โดเมนการค วาคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สามารถช่วยลูกค้าวิเคราะห์และประเมินเหตุการณ์ความ ปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น และประเมินความเสี่ยงด้านการเปิดเผยสินทรัพย์ขององ ค์หรือองค์กรของคุณมากขึ้น สนับสนุนองค์กรในการสร้างระบบป้องกันความปลอดภัย แบบสามมิติที่มีประสิทธิภาพ ศูนย์ข่าวกรองภัยคุกคามยังสามารถรวมเข้ากับผลิตภัณฑ์ เพื่อป้องกันความปลอดภัยที่มีอยู่ของลูกค้าได้ในรูปแบบ การรวมเข้าด้วยกัน เพื่อเชื่อมโยงข้อมูลข่าวกรองจากคลาวด์กับผลิตภัณฑ์ ดังกล่าว เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัย โดยรวมและการตอบสนองต่อภัยคุกคาม ด้วยการเสริมพลังและการสนับสนุนจากศูนย์ข่าวกรอง ภัยคุกคาม Tencent Cloud มุ่งมั่นที่จะสร้างระบบความสามารถด้านความปลอดภัยใ นการป้องกันเชิงรุกแบบ "ข่าวกรอง- การโจมตีและการป้องกัน-การจัดการ-การวางแผน" โดยบูรณาการเทคโนโลยีต่างๆ เช่น ข่าวกรองภัยคุกคาม ปัญญาประดิษฐ์ ข้อมูลขนาดใหญ่ เพื่อเพิ่มความสามารถและประสิทธิภาพในการตอบสนอง ต่อเหตุการณ์ความปลอดภัย และได้จัดตั้งศูนย์ปฏิบัติการความปลอดภัยที่ทำงาน 24 ชั่วโมงทุกวัน ให้มีความสำคัญกับการตรวจจับภัยคุกคาม การสอบสวน และการตอบสนอง เพื่อให้บรรลุความสามารถในการรับรู้ มองเห็น และควบคุมสถานการณ์ความปลอดภัย สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบความปลอด ภัย โปรดดูเนื้อหาในข้อ "6.5 ติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีส วสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
8	การเก็บคืนและ การทำลายข้อมูล เมื่อสิ้นสุดการใ ้บริการ	เมื่อสิ้นสุดหรือยกเลิกการใช้บริการ cloud computing ในระบบงานที่มีนัยสำคัญจากบุคคล ภายนอก สถาบันการเงินและสถาบันการเงินเ นเฉพาะกิจต้องนำข้อมูลของสถาบันก	ลูกค้าควรกำหนดขั้นตอนการยกเลิกหรือสิ้นสุดสัญญา หรือข้อตกลง กำหนดกลยุทธ์และแผนการยุติการให้บริการให้ชัดเจน เพื่อให้แน่ใจว่าผู้ให้บริการภายนอกได้ทำลายหรือลบขอ มูลที่เกี่ยวข้องทั้งหมดอย่างสิ้นเชิง

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		การเงินและสถาบันการเงินเฉพาะกิจ หรือข้อมูลของลูกค้ากลับมาจากบุคคลภายนอก และลบหรือทำลายข้อมูลทั้งหมดที่อยู่กับบุคคลภายนอก อย่างครบถ้วน โดยบุคคลภายนอกต้องไม่สามารถกู้คืนข้อมูลได้	และไม่สามารถกู้คืนได้ หากลูกค้าจำเป็นต้องยกเลิกข้อตกลงตามสัญญาเนื่องจากมีการเปลี่ยนแปลงธุรกิจหรือการวางแผนเทคโนโลยีสารสนเทศในอนาคต ลูกค้าสามารถเลือกทำการสำรองข้อมูลและย้ายข้อมูลและสภาพแวดล้อมการผลิตบนคลาวด์ได้ทุกเวลา ผลิตภัณฑ์คลาวด์ที่ ตามข้อตกลงการให้บริการระหว่าง Tencent Cloud กับลูกค้า หากบริการคลาวด์หมดอายุหรือสิ้นสุดลง สำหรับข้อมูลที่ลูกค้าเก็บไว้ในเซิร์ฟเวอร์คลาวด์เนื่องจากการใช้บริการ Tencent Cloud ลูกค้าจำเป็นต้องทำการย้ายข้อมูลให้เสร็จสิ้นก่อนช่วงเวลาเก็บข้อมูลสิ้นสุดลง Tencent Cloud ให้มารองรับให้ลูกค้าใช้รูปแบบมาตรฐานทั่วไปเพื่อสำรองและย้ายข้อมูลของลูกค้า และลูกค้าสามารถใช้วิธีการส่งและโปรโตคอลการส่งเดียวกันกับขั้นตอนการย้ายขึ้นคลาวด์ หรือใช้บริการเครือข่าย เช่น Direct Connect (DC) VPN Connection เพื่อให้มั่นใจว่าข้อมูลของลูกค้าในขั้นตอนการย้ายออกจากคลาวด์มีความปลอดภัยและเชื่อถือได้ เมื่อบริการคลาวด์สิ้นสุดลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยจะลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรองอย่างสิ้นเชิงหลังจากช่วงเวลาเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้
9	ความต่อเนื่องทางธุรกิจและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ	แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ครอบคลุมการใช้บริการ cloud computing ในระบบงานที่มีนัยสำคัญจากบุคคลภายนอก โดยควรคำนึงถึงเหตุการณ์ที่อาจส่งผลกระทบรุนแรงหรือเลวร้ายที่สุด (worst case scenario) อย่างน้อยครอบคลุมเหตุการณ์ ดังนี้ (1) ระบบงานของบุคคลภายนอกใน region ที่ใช้บริการอยู่หยุดชะงักจนเป็นเหตุ	ลูกค้าควรสร้างกลไกการจัดการความต่อเนื่องของธุรกิจ จัดทำแผนความต่อเนื่องของธุรกิจที่ครอบคลุมบริการภายนอก ดำเนินการวิเคราะห์ผลกระทบทางธุรกิจ กำหนดเป้าหมายเวลาในการกู้คืน (RTO) และเป้าหมายจุดข้อมูลในการกู้คืน (RPO) ของแต่ละธุรกิจให้ชัดเจน จัดทำแผนฉุกเฉินเพื่อความต่อเนื่องของธุรกิจ และสื่อสารไปยังผู้ที่เกี่ยวข้อง นอกจากนี้ ลูกค้ายังควรตรวจสอบและทดสอบการดำเนินการตามแผนฉุกเฉินอย่างน้อยปีละครั้ง เพื่อให้มั่นใจว่าลูกค้าสามารถตอบสนองและกู้คืนฟังก์ชันสำคัญได้อย่างรวดเร็วหลังเกิดเหตุการณ์ภัยพิบัติ ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ให้บริการของสถาบัน การเงินและสถาบันการเงินเฉพาะกิจ ไม่สามารถให้บริการได้อย่างต่อเนื่อง เช่น hardware และ software ที่สถาบันการเงินและสถาบันการเงิน เฉพาะกิจใช้บริการจากบุคคลภายนอก ได้รับเสียหาย ทั้งหมด management console ถูกโจมตี เป็นต้น	ให้มา เช่น บริการคอมพิวเตอร์ บริการเครือข่าย บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ บริการความปลอดภัย ล้วนมีคุณสมบัติและความพร้อมใช้งานสูง และมีแผนการกู้คืนจากภัยพิบัติที่สอดคล้องกัน
	(2)ระบบงานของบุคคลภายนอกทุก region	หยุดชะงักจนเป็นเหตุให้บริการของส ถาบันการเงินและสถาบัน การเงินเฉพาะกิจไม่สามารถให้บริการ ได้อย่างต่อเนื่อง	เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการก ากับดูแล Tencent Cloud มีการแยกจากกันโดยสมบูรณ์ระหว่างภูมิภาคต่างๆ เพื่อรับประกันความเสถียรและความทนทานต่อข้อผิดพลาด สูงสุดระหว่างภูมิภาคต่างๆ
	(3)สายสื่อสารระหว่างสถาบันการ เงินและสถาบันการเงินเฉพาะกิจ และบุคคลภายนอกขัดข้องทุกช่องท าง จนไม่สามารถใช้บริการได้		เพื่อให้มั่นใจในความพร้อมใช้งานสูงของข้อมูล Tencent Cloud แบ่งแต่ละภูมิภาคออกเป็นหลาย Availability Zone ที่แยกจากกัน การออกแบบหลาย Availability Zone ของ Tencent Cloud สามารถลดผลกระทบจากความล้มเหลวของจุดเดียวได้ อย่างมีประสิทธิภาพ และรับประกันว่าความล้มเหลวระหว่าง Availability Zone จะถูกแยกจากกัน ซึ่งจะช่วยรับประกันความต่อเนื่องของธุรกิจของลูกค้า Tencent Cloud ได้รับการรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจแล้ว Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิต ภัณฑ์และบริการคลาวด์ และจัดทำกลยุทธ์การตอบสนองที่แตกต่างกัน แผนความต่อเนื่องของธุรกิจ และแผนการกู้คืนจากภัยพิบัติตามผลการวิเคราะห์ เพื่อขึ้นำองค์กรในการกู้คืนทรัพยากรทางธุรกิจที่เกี่ยวข้อง ของ Tencent Cloud ได้จัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดย ละเอียดสำหรับผลิตภัณฑ์คลาวด์ และดำเนินการฝึกซ้อมตามแผนกู้คืนจากภัยพิบัตินั้น อย่างเคร่งครัดตามข้อกำหนดเป็นประจำ เพื่อรับประกันความทันเวลาความเป็นไปได้ของแผนกู้ คืนจากภัยพิบัติ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความต่อเนื่องของธุรกิจแ ละแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โปรดดูเนื้อหาในข้อ "9.1-9.6 การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการค วบรวม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ศ" ของ " <u>5.3 เอกสารแนบ 2</u> <u>การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีส</u> <u>สารสนเทศ</u> <u>ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ</u> ในคู่มือนี้

06

Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ
หลักเกณฑ์การให้บริการจาก
ผู้ให้บริการภายนอก ของ
BOT อย่างไร

BOT No. FPG 8/2557 เรื่อง หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing)

ได้กำหนดหลักเกณฑ์ของธนาคารแห่งประเทศไทยในการเลือกผู้ให้บริการสำหรับสถาบันการเงิน พร้อมทั้งระบุแนวทางปฏิบัติที่ดีเพื่อลดความเสี่ยงจากการจ้างทำภายนอกและปกป้องลูกค้าสถาบันการเงินจากผลกระทบที่ไม่พึงประสงค์ที่เกี่ยวข้องกับการจ้างทำภายนอก

ข้อกำหนดหลักครอบคลุมการจำแนกประเภทงานจ้างทำภายนอก การขอใบอนุญาตจ้างทำภายนอก การตรวจสอบโดยธนาคารแห่งประเทศไทย ผู้สอบบัญชีภายนอก หรือหน่วยงานกำกับดูแลอื่นๆ และการรายงานต่อธนาคารแห่งประเทศไทย เป็นต้น

ระเบียบบริหารดังกล่าวได้จัดทำและเผยแพร่ภาคผนวก 3

ซึ่งกำหนดให้สถาบันการเงินประเมินสถานะการดำเนินงานและประสิทธิผลของการจัดการความเสี่ยงที่เกี่ยวข้องกับกิจกรรมการจ้างทำภายนอกโดยรวม

ตามแนวทางการกำกับดูแลการจ้างทำภายนอกในภาคผนวก 3

ในบทนี้ Tencent Cloud

จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จากภาคผนวก 3 ของ

หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก (Outsourcing)

และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud

จะช่วยสถาบันการเงินในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ 3-2	การคัดเลือก ผู้ให้บริการภายนอก	สถาบันการเงินจะต้องกำหนดแนวทาง การคัดเลือกผู้ให้บริการภายนอกอย่าง เหมาะสม	ลูกค้าควรกำหนดเกณฑ์ในการเลือกผู้ให้บริการให้ชัดเจนก่อนการลงนามในสัญญาใหม่หรือต่ออายุสัญญา โดยครอบคลุมประเด็นหลักดังต่อไปนี้:
		ก่อนที่จะทำสัญญาใหม่หรือทบทวนเพื่ ต่ออายุสัญญาการใช้บริการจากผู้ให้ บริการภายนอกรายเดิม	ความสามารถทางเทคนิคและความเชี่ยวชาญ ความมั่นคงทางการเงิน ชื่อเสียงทางธุรกิจ วัฒนธรรมองค์กรที่สอดคล้องกับสถาบันการเงิน
		โดยต้องพิจารณาให้ครอบคลุมประเดี นสำคัญอย่างน้อย ดังต่อไปนี้	ความสามารถในการปรับตัวต่อการพัฒนาใหม่ๆ ความเสี่ยงด้านความเข้มข้น (concentration risk)
		(1)ความสามารถทางด้านเทคนิค ความเชี่ยวชาญ และประสิทธิภาพในการดำเนินงาน	รวมถึงข้อกำหนดที่ชัดเจนเกี่ยวกับการมอบหมายงานด้ านที่เกี่ยวข้องกับคณะกรรมการและผู้บริหารระดับสูงให้ กับผู้ให้บริการภายนอก
		(2)สถานะความมั่นคงทางการเงิน	Tencent Cloud ได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและส ับสนุนกิจกรรมการตรวจสอบอย่างละเอียดของลูกค้า อย่างเข้มข้น ต่อไปนี้เป็นภาพรวมของ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ในด้านต่างๆ ของการตรวจสอบอย่างละเอียด:
		(3)ชื่อเสียงทางธุรกิจ ประวัติการถูกร้องเรียน หรือถูกฟ้องร้องดำเนินคดี	• ความสามารถทางวิชาชีพและทางเทคนิค :
		(4)วัฒนธรรมองค์กรและนโยบายการใ ้บริการที่มีความเหมาะสมกับสถาบัน การเงิน	
		(5)ความสามารถในการปรับตัวตอบส อนงพัฒนาการใหม่ ๆ	Tencent Cloud ได้แสดงความสามารถทางเทคนิคที่ครอบคลุมในฐานะผู้ นำในอุตสาหกรรมผ่านเทคโนโลยีคอมพิวเตอร์คลาวด์ ที่แข็งแกร่ง
		(6)ความเสี่ยงในกรณีที่ผู้ให้บริการภา ยนอกให้บริการแก่สถาบันการเงินหลา	

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ยแห่ง (Concentration risk) (7)หลักเกณฑ์ที่ชัดเจนเกี่ยวกับการพิจารณาการใช้บริการจากผู้ให้บริการรายนอก ที่มีส่วนเกี่ยวข้องกับคณะกรรมการและผู้บริหารระดับสูง	ความสามารถในการประมวลผลข้อมูลขนาดใหญ่ การประยุกต์ใช้ปัญญาประดิษฐ์ การป้องกันความปลอดภัยทางไซเบอร์ เทคโนโลยีคลาวด์เนทีฟ การกระจายตัวของศูนย์ข้อมูลทั่วโลก และโซลูชันอุตสาหกรรม ความสามารถทางเทคนิคเหล่านี้ไม่เพียงรับประกันความมั่นคงและความน่าเชื่อถือของบริการ Tencent Cloud เท่านั้น แต่ยังจัดเตรียมสภาพแวดล้อมคอมพิวเตอร์คลาวด์ที่ปลอดภัยและน่าเชื่อถือให้กับลูกค้าด้วย ความสามารถด้านความปลอดภัยในการดำเนินงานที่ครบถ้วนของ Tencent Cloud ยังสามารถให้การสนับสนุนทางเทคนิครอบนาฬิกาสำหรับผลิตภัณฑ์คลาวด์แก่ลูกค้าได้ ประสบการณ์ในการดำเนินงาน: ความสามารถในการดำเนินงานและขนาดของ Tencent Cloud อยู่ในตำแหน่งผู้นำในอุตสาหกรรมศูนย์ข้อมูลของ Tencent Cloud มีการกระจายตัวอยู่ในหลายภูมิภาคทั่วโลก ครอบคลุมพื้นที่จีนแผ่นดินใหญ่ ภูมิภาคเอเชียแปซิฟิก ภูมิภาคอเมริกาเหนือ และภูมิภาคยุโรป สภาพทางการเงิน: Tencent Cloud ซึ่งเป็นแบรนด์คอมพิวเตอร์คลาวด์ที่ Tencent Group สร้างขึ้นด้วยความอดสาหะ ได้รับประโยชน์จากความแข็งแกร่งทางการเงินและสภาพทางการเงินที่มั่นคงของ Tencent Group นับตั้งแต่ปี 2010 ที่ Tencent Cloud เริ่มให้บริการคลาวด์แก่สาธารณะอย่างเป็นทางการ Tencent Cloud ได้บรรลุแนวโน้มการเติบโตที่โดดเด่นในตัวชี้วัดทางการเงินที่สำคัญ เช่น รายได้และผลกำไร Tencent Cloud ได้รับการยอมรับจากสถาบันวิจัยอุตสาหกรรมระดับโลก ยกขึ้นนำ Gartner ติดต่อกันเป็นเวลาสี่ปี โดยอยู่ในอันดับที่สองในด้านมิติด้านกลยุทธ์ในหมวดผู้ผลิตจากประเทศจีน ชื่อเสียงทางธุรกิจ: ในฐานะแบรนด์คอมพิวเตอร์คลาวด์ภายใต้การนำของ Tencent ซึ่งเป็นบริษัทชั้นนำในอุตสาหกรรมอินเทอร์เน็ตของจีน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Tencent Cloud ได้รับการรับรองจากสถาบันอุตสาหกรรมหลายแห่ง มอบโซลูชันคอมพิวเตอร์คลาวด์ที่ครอบคลุม และได้ร่วมมือกับพันธมิตรมากกว่า 11,000 ราย เพื่อมอบโซลูชันอุตสาหกรรมมากกว่า 400 รายการให้กับลูกค้าธุรกิจในกว่า 30 อุตสาหกรรม วัฒนธรรมองค์กรและนโยบายการให้บริการ ที่มีความเหมาะสมกับสถาบันการเงิน: Tencent Cloud สามารถปรับโซลูชันให้เหมาะสมตามความต้องการของ ลูกค้า ปรับตัวได้อย่างยืดหยุ่นกับวัฒนธรรมและกลยุทธ์ขององ ค์กรที่แตกต่างกัน Tencent Cloud ได้ปรับแต่งโซลูชันต่างๆ ให้เหมาะสมสำหรับสถาบันการเงินหลายแห่ง มอบบริการคลาวด์เฉพาะสำหรับการเงินที่สอดคล้องกับ ข้อกำหนดด้านกฎระเบียบให้กับลูกค้าทางการเงินหล ายราย และมีขีดความสามารถในการปฏิบัติตามข้อกำหนดด้าน ความปลอดภัยระดับการเงิน ความสามารถในการปรับตัวต่อพัฒนาการ ใหม่: Tencent Cloud ติดตามแนวโน้มตลาดและการพัฒนาทางเทคโนโลยีอย างเข้มข้น ออกผลิตภัณฑ์และบริการใหม่ๆ อย่างต่อเนื่อง เพื่อรักษาตำแหน่งผู้นำในตลาดและตอบสนองความต้อ งการล่าสุดของลูกค้า การจัดการความเสี่ยง: Tencent Cloud ได้กำหนดกรอบการกำกับดูแลความเสี่ยงและขั้นตอนที่ เกี่ยวข้อง และปรับปรุงมาตรการจัดการความเสี่ยงและระบบตรวจ สอบภายในอย่างต่อเนื่อง โดยการเสริมสร้างวัฒนธรรมความเสี่ยงอย่างต่อเนื่อง Tencent Cloud ปรับปรุงความสามารถในการจัดการความเสี่ยงภายใน อย่างมีประสิทธิภาพ และรับประกันการพัฒนาทางธุรกิจที่ยั่งยืนและมีสุขภา พดี

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสาร แนบ 3-3 (1)	ความปลอดภัย และการรักษา ความลับของ ข้อมูล	(1) ต้องดูแลให้ผู้ให้บริการภายนอกจัดให้มีระบบรักษาความปลอดภัยและรักษาความลับ ข้อมูลของลูกค้า และข้อมูลของสถาบันการเงินเป็นอย่างดี เช่น	ลูกค้าควรเชื่อมั่นให้ผู้ให้บริการสร้างระบบที่เกี่ยวข้องเพื่อรักษาความปลอดภัยและความเป็นส่วนตัวของลูกค้าและข้อมูลสถาบันการเงิน
		การแบ่งแยกข้อมูลของลูกค้าของสถาบัน การเงิน ออกจากข้อมูลของผู้ให้บริการภายนอกหรือข้อมูลของลูกค้ารายอื่นของผู้ให้บริการภายนอก การกำหนดสิทธิการเข้าถึงข้อมูลของพนักงานของผู้ให้บริการภายนอกอย่างเข้มงวด (Data access control) รวมทั้งต้องตรวจสอบระบบดังกล่าวอย่างเหมาะสม และดูแลให้ผู้ให้บริการภายนอกควบคุมดูแล พนักงานอย่างเข้มงวดในการรักษาความลับข้อมูลของลูกค้าและข้อมูลของสถาบันการเงิน	ในด้านการปฏิบัติตามข้อกำหนดข้อมูล Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัดในการปกป้องความเป็นส่วนตัวของผู้ใช้และความปลอดภัยของข้อมูล ดำเนินการตามมาตรฐานและมาตรการป้องกันความเป็นส่วนตัวขั้นนำระดับโลกอย่างเข้มข้น สร้างระบบการจัดการความปลอดภัยข้อมูลและการปกป้องความเป็นส่วนตัวที่สมบูรณ์ และได้รับใบรับรองมาตรฐานสากลหลายรายการ ในด้านการแยกผู้เช่า Tencent Cloud ปฏิบัติตามหลักการ "ความเป็นส่วนตัวของข้อมูล" อย่างเคร่งครัด โดยใช้นโยบายการควบคุมการเข้าถึงทรัพยากรในชั้นควบคุมการทำให้เป็นเสมือนจริง (Virtualization Control Layer) นโยบายการแยกเครือข่ายส่วนตัวภายในแพลตฟอร์มคลาวด์ การจัดสรรสิทธิ์และยืนยันตัวตนบนเว็บคอนโซลรหัสเซสชันของอินเทอร์เน็ตพีชและศักยภาพการเข้าถึงและกลไกความปลอดภัยอื่นๆ เพื่อให้แน่ใจว่าข้อมูลของลูกค้าไม่สามารถมองเห็นซึ่งกันและกัน และรับประกันว่าผู้เช่าไม่สามารถเข้าถึง รับหรือแก้ไขข้อมูลของผู้เช่าอื่นได้ Tencent Cloud ยังจัดเตรียมบริการต่างๆ เช่น Virtual Private Cloud (VPC) และ Cloud Firewall (CFW) เพื่อช่วยลูกค้าเสริมสร้างความเข้มงวดในการแยกเครือข่ายและการป้องกันขอบเขตเครือข่ายเพิ่มเติม ในด้านการปกป้องข้อมูล ข้อมูลของลูกค้าภายใน Tencent Cloud จัดอยู่ในระดับความปลอดภัยสูง ลูกค้ามีความเป็นเจ้าของและการควบคุมสิทธิ์เหนือเนื้อหาข้อมูลของตนโดยสมบูรณ์ เว้นแต่มีความจำเป็นในการให้บริการหรือแก้ไขข้อบกพร่อง และได้รับอนุญาตจากลูกค้าอย่างชัดเจน หรืออยู่ในสถานการณ์การสืบสวนคดีอาญาโดยหน่วยงานภาครัฐระดับชาติหรือท้องถิ่นซึ่งสอดคล้องกับกฎหมายและระเบียบข้อบังคับของประเทศ พนักงานภายในของ Tencent Cloud จะไม่สัมผัสข้อมูลลูกค้าใดๆ อย่างเข้มข้น Tencent

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Cloud ใช้ระบบตรวจสอบและบำรุงรักษาการยืนยันตัวตนด้วย ชื่อจริงแบบเต็มทุกโหนดสำหรับสิทธิ์การเข้าถึงข้อมูล เพื่อรับประกันความสมบูรณ์ของสินทรัพย์ข้อมูลและคว ามน่าเชื่อถือของบริการธุรกิจ และได้สร้างกลไกการตรวจสอบและล็อกแบบเรียลไทม์ เพื่อตรวจจับและป้องกันพฤติกรรมการณ์เข้าถึงข้อมูลที่ผิด ปกติใดๆ พร้อมทั้งได้ลงนามข้อตกลงการรักษาความลับกับพนัก งาน เพื่อปกป้องข้อมูลของลูกค้า ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการ ของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็ง แกร่งสูง และผสานรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล
เอกสาร แนบ 3-3 (2)	การจัดการปี งฎา	(2)ต้องจัดให้มีระบบดูแลเรื่องร้องเรียน และแก้ปัญหาแก่ลูกค้าอย่างเพียงพอเอ เหมาะสม โดยต้องมีการบันทึกและติดตามข้อมูล ข้อร้องเรียนจากลูกค้า ซึ่งรวมถึงประเด็นปัญหาจากการรั่วไห ล ของข้อมูลส่วนบุคคลของลูกค้า ทั้งนี้ สถาบันการเงินต้องก าหนดแนวทางที่เหมาะสมในการแก้ไข ปัญหาดังกล่าว และรายงานข้อมูลต่อผู้บริหารระดับสูง ของสถาบันการเงินให้ทราบเป็นระยะ	ลูกค้าควรสร้างกลไกที่เหมาะสมเพื่อบันทึกและตรวจสอบ บข้อร้องเรียนของลูกค้า และจัดทำกลไกการตอบสนองและการจัดการสำหรับปี ญหาดังกล่าว ข้อมูลที่เกี่ยวข้องควรรายงานต่อผู้บริหารระดับสูงเป็นเป ระจำ เพื่อสนับสนุนลูกค้าในการตรวจจับและตอบสนองต่ออ บัติเหตุอย่างรวดเร็ว Tencent Cloud ให้บริการแพลตฟอร์มการจัดการความปลอดภัยแบบค บวงจร Cloud Security Center (CSC) ผ่านฟังก์ชันต่างๆ เช่น ศูนย์สินทรัพย์ ศูนย์ความเสี่ยง ศูนย์แจ้งเตือน และการจัดการความปลอดภัยขั้นสูง ช่วยลูกค้าบรรลุล่วงจรรยาบรรณด้านความปลอดภัย ได้แก่ การตรวจจับภัยคุกคามก่อนเกิดเหตุ การตอบสนองและจัดการระหว่างเกิดเหตุ และการวิเคราะห์ย้อนหลังหลังเหตุการณ์ เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัย ในด้านการจัดการเหตุการณ์ Tencent Cloud ได้กำหนดขั้นตอนการจัดการเหตุการณ์และคำขอรับบ ริการภายในองค์กร และสร้างกลยุทธ์การจัดการเหตุการณ์ของ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อให้มั่นใจว่าเหตุการณ์ที่เกี่ยวข้องกับกิจกรรมการจัด การบริการเทคโนโลยีสารสนเทศได้รับการบันทึกและจำ แนกประเภท และจัดลำดับความสำคัญตามผลกระทบและความเร่งด่วน รวมถึงการยกระดับตามความจำเป็น เพื่อแก้ไขและปิดเหตุการณ์ทุกประเภทอย่างรวดเร็ว ทำให้ผลกระทบของเหตุการณ์มีน้อยที่สุด รักษาการดำเนินธุรกิจให้เป็นปกติ และเพิ่มความพึงพอใจของลูกค้า ในด้านการสื่อสารและการแจ้งเหตุการณ์ Tencent Cloud ได้กำหนดมาตรฐานการจัดการเหตุการณ์ความปลอดภัย ภัยข้อมูล สร้างขั้นตอนที่เกี่ยวข้อง เช่น การตอบสนองเหตุการณ์ความปลอดภัยข้อมูล การยกระดับเหตุการณ์ และการแจ้งเหตุการณ์ เพื่อแจ้งเตือนหรือแจ้งให้พนักงานภายในบริษัท ลูกค้า และผู้เกี่ยวข้องอื่น ๆ ที่อาจหรือได้รับผลกระทบจากอุบัติเหตุทราบทันเวลา ทำให้ทุกฝ่ายสามารถสื่อสารและประสานงานกันอย่าง เป็นระเบียบ ทันเวลา และมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบ ต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัย ข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียใ ห้เหลือน้อยที่สุด ในด้านการที่ลูกค้าแจ้งปัญหาหรือติดต่อ Tencent Cloud คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการในงาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับ ระบบในงานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับในงานของลูกค้าผ่านกลไ กการตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			รูปภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติโดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมและจัดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้าได้รับการตอบสนองและจัดการอย่างทันทางที่ นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาคสามารถจัดการข้อซักถามหรือความต้องการจากลูกค้าได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเวล ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับการสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า
เอกสารแนบ 3-3 (3) (4)	การจัดการต้นทุน	(3) ต้องไม่ทำให้คุณภาพของบริการที่ลูกค้าได้รับด้อยลงหรือผลกระทบค่าใช้จ่ายทั่วไป ที่เกิดขึ้นเป็นประจําอยู่แล้วของสถาบันการเงินไปให้แก่ลูกค้า ตลอดจนการใช้บริการดังกล่าวต้องไม่เ ป็น อุปสรรคต่อการปฏิบัติตามกฎหมายระเบียบ และข้อบังคับของทางการ (4) ต้องเปิดเผยข้อมูลที่อาจมีผลกระทบต่อกลูกค้าให้ทราบล่วงหน้า (Information disclosure) จากการมอบหมายให้ผู้ให้บริการภายนอกดำเนินการแทนสถาบันการเงิน เช่น ค่าธรรมเนียม หรือค่าบริการ	ลูกค้าควรให้ความมั่นใจว่าคุณภาพการบริการแก่ลูกค้าของตนจะไม่ลดลง และไม่มีการโอนย้ายภาระต้นทุนไปยังลูกค้าของตนเองในเวลาเดียวกัน หากลูกค้ามอบหมายให้ผู้ให้บริการดำเนินการแทนตนควรเปิดเผยข้อมูลที่เกี่ยวข้อง เช่น ค่าธรรมเนียมและค่าบริการ ให้ลูกค้าของตนทราบล่วงหน้า บริการคลาวด์ที่ Tencent Cloud มอบให้แก่ลูกค้ามีการส่งมอบตามข้อตกลงระดับการให้บริการ (SLA) ที่ตกลงกันสำหรับแต่ละบริการ ตัวชี้วัดประสิทธิภาพ เกณฑ์การวัด และข้อกำหนดในการรายงานสำหรับบริการแต่ละรายการกำหนดไว้อย่างชัดเจนใน SLA ของผลิตภัณฑ์แต่ละรายการ และเผยแพร่บนเว็บไซต์อย่างเป็นทางการของ Tencent Cloud Tencent Cloud จะติดตามประสิทธิภาพและความพร้อมใช้งานของบริการคลาวด์อย่างต่อเนื่อง และให้การตรวจสอบแบบเรียลไทม์แก่ลูกค้าผ่านคอนโซลการจัดการ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ลูกค้าสามารถตรวจสอบยอดเงินคงเหลือที่ใช้ได้ของบัญชี รายละเอียดรายรับรายจ่าย ข้อมูลค่าใช้จ่ายที่เกิดจากการใช้บริการ Tencent Cloud ผ่านศูนย์ค่าใช้จ่ายในคอนโซล Tencent Cloud
เอกสาร รแนบ 3-3 (5)	การลบข้อมูล ลูกค้า	(5) ในกรณีการสิ้นสุดหรือยกเลิกสัญญาว่าจ้างผู้ให้บริการภายนอกไม่ว่าด้วยสาเหตุใด สถาบันการเงินต้องดำเนินการเพื่อให้แน่ใจว่าข้อมูลของลูกค้าได้ถูกทำลายหรือได้นำข้อมูลทั้งหมด ของลูกค้ากลับมาจากผู้ให้บริการภายนอกแล้ว	หากลูกค้ายกเลิกหรือสิ้นสุดสัญญากับผู้ให้บริการ ควรให้มั่นใจว่าผู้ให้บริการจะทำลายหรือลบข้อมูลที่เกี่ยวข้องทั้งหมด หากลูกค้าจำเป็นต้องยกเลิกข้อตกลงตามสัญญาเนื่องจากมีการเปลี่ยนแปลงธุรกิจหรือการวางแผนเทคโนโลยีสารสนเทศในอนาคต ลูกค้าสามารถเลือกทำการสำรองข้อมูลและย้ายข้อมูลและสภาพแวดล้อมการผลิตบนคลาวด์ได้ทุกเวลา ผลิตภัณฑ์คลาวด์ที่ เมื่อบริการคลาวด์สิ้นสุดลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยจะลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรองอย่างสิ้นเชิงหลังจากช่วงเวลาเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้
เอกสาร รแนบ 3-3 (6)	การปฏิบัติตาม กฎหมายและ ระเบียบข้อบังคับ	(6) ต้องดูแลข้อมูลของลูกค้าหรือข้อมูลของสถาบันการเงินเอง ให้เป็นไปตามที่บัญญัติไว้ในกฎหมายว่าด้วยธุรกิจสถาบันการเงิน และกฎหมายอื่นที่เกี่ยวข้อง	ลูกค้าควรให้มั่นใจว่าผู้ให้บริการปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับธุรกิจของสถาบันการเงิน Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด และได้สร้างขั้นตอนที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านความปลอดภัย เพื่อให้มั่นใจว่าการดำเนินการด้านความปลอดภัยข้อมูลเป็นไปตามข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ มาตรฐาน และขั้นตอนที่เกี่ยวข้อง ทีมงานฝ่ายกฎหมายของ Tencent Cloud จะระบุและรวบรวมข้อกำหนดการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับธุรกิจของ Tencent Cloud อย่างต่อเนื่อง จัดทำเป็นรายการกฎหมายและระเบียบข้อบังคับที่สอดคล้องกัน และบำรุงรักษาและปรับปรุงเป็นประจำ
เอกสาร รแนบ 3-4	การบริหารคว ามต่อเนื่องทาง ธุรกิจ (Business	(1) สถาบันการเงินต้องระบุความสำคัญของกลุ่มงานที่ใช้บริการจากผู้ให้บริการภายนอก โดยประเมินความเสี่ยงและผลกระทบที่	ลูกค้าควรดำเนินการประเมินความเสี่ยงสำหรับบริการเพื่อกำหนดระดับความสำคัญของกิจกรรมการจ้างทำภายนอก และควรกำหนดให้ผู้ให้บริการจัดทำแผนความต่อเนื่อง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
	continuity manageme nt) ของผู้ให้บริการ ภายนอก	อาจเกิดขึ้นจากการหยุดชะงักของงาน นั้น (2)สถาบันการเงินต้องกำหนดให้ผู้ให้ บริการภายนอกจัดทำแผนรองรับการ ดำเนินธุรกิจ อย่างต่อเนื่อง (Business continuity plan) โดยเฉพาะส หรับกรณีที่เกิดการหยุดชะงักของงาน สำคัญ (Significant activity) หรืองานที่มีผลกระทบต่องานบริการใน วงกว้าง (Wide impact) พร้อมทั้ง จัดสรรทรัพยากรรองรับการดำเนินงาน อย่างเพียงพอ โดยอ้างอิงจากหลักเกณฑ์ของธนาคาร แห่งประเทศไทย ว่าด้วยการบริหารความต่อเนื่องทางธุรกิจ (Business continuity management: BCM) และการจัดทำ แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business continuity plan: BCP) ของสถาบันการเงิน ในระดับ ที่สามารถที่จะกำหนดแผนรองรับการ ดำเนินธุรกิจอย่างต่อเนื่องของสถาบัน การเงินเองให้สอดคล้องกันได้ ทั้งนี้ สถาบันการเงินต้องจัดให้มีการทดสอบ แผนรองรับการด ำเนินธุรกิจอย่างต่อเนื่อง ร่วมกับผู้ให้บริการภายนอกหลัก (Key service provider) อย่างสม่ำเสมอ และต้องมีการบันทึกผล การทดสอบไว้เป็นเอกสารเพื่อให้ธนาคาร แห่งประเทศไทยสามารถตรวจสอบได้	ทางธุรกิจ และหากจำเป็น ให้ทดสอบแผนความต่อเนื่องทางธุรกิจกับผู้ให้บริการที่ สำคัญเป็นประจำ Tencent Cloud ได้สร้างระบบการจัดการความต่อเนื่องทางธุรกิจและการ กู้คืนจากภัยพิบัติที่ครอบคลุมภายในองค์กร และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องทางธุรกิจแล้ว เพื่อให้มั่นใจในความพร้อมใช้งานอย่างต่อเนื่องของ ธุรกิจลูกค้า Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิต ภัณฑ์และบริการคลาวด์ กำหนด RTO และ RPO ของแต่ละธุรกิจให้ชัดเจน และจัดทำกลยุทธ์การตอบสนองและแผนความต่อเนื่อง ของธุรกิจที่แตกต่างกันตามผลการวิเคราะห์ผลกระทบ ทางธุรกิจ รวมถึงจัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโ ดยะเอียดสำหรับผลิตภัณฑ์คลาวด์ กลยุทธ์ แผนการ และแผนฉุกเฉินที่เกี่ยวข้องครอบคลุมทุกด้าน เช่น สถานที่ บุคลากร อุปกรณ์ ระบบ ข้อมูล/สารสนเทศ และลำดับความสำคัญของธุรกิจ Tencent Cloud จัดทำแผนการฝึกซ้อมโดยอิงตามแผนความต่อเนื่องขอ งธุรกิจ และดำเนินการประเมินความเสี่ยงในการฝึกซ้อม พร้อมกำหนดมาตรการรับประกันที่สอดคล้องกัน เพื่อหลีกเลี่ยงผลกระทบเชิงลบต่อบริการจากการฝึกช ้อม การฝึกซ้อมการกู้คืนจากภัยพิบัติของ Tencent Cloud มักดำเนินการโดยจำลองสถานการณ์การกู้คืนจากภัย พิบัติแบบคลาสสิกที่สมจริง รวมถึงการต่อสู้ป้องกันการโจมตีและความล้มเหลวขนาด ใหญ่ เพื่อตรวจสอบความสามารถในการกู้คืนจากภัยพิบัติข องระบบ ความเร็วในการตอบสนอง และความสามารถในการกู้คืนอย่างครอบคลุมหลังการฝึ กซ้อมเสร็จสิ้น หน่วยงานที่เกี่ยวข้องจัดทำรายงานการฝึกซ้อม ดำเนินการแก้ไขตามมาตรการปรับปรุง และเก็บรายงานไว้เป็นเอกสาร หากลูกค้าประเมินว่าการฝึกซ้อมการกู้คืนจากภัยพิบัติ จำเป็นต้องได้รับการมีส่วนร่วมและความร่วมมือจากฝาย Tencent Cloud Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะตอบสนองอย่างแข็งขันและให้ความร่วมมืออย่างเต็มที่ เราจะกำหนดสถานการณ์และขอบเขตการฝึกซ้อมให้ชัดเจนตามความต้องการเฉพาะของลูกค้า ร่วมจัดทำแผนการฝึกซ้อมและแผนการดำเนินการโดยละเอียด ให้การสนับสนุนทางเทคนิคและการประสานทรัพยากรที่จำเป็นระหว่างกระบวนการฝึกซ้อม และช่วยลูกค้าเพิ่มประสิทธิภาพกลยุทธ์และขั้นตอนการกู้คืนจากภัยพิบัติอย่างต่อเนื่อง เพื่อร่วมกันยกระดับความสามารถในการต่อเนื่องของธุรกิจและการกู้คืนจากภัยพิบัติ
เอกสารแนบ 3-5	สัญญาและข้อตกลง	สถาบันการเงินต้องทำสัญญาและข้อตกลงกับผู้ให้บริการภายนอกเป็นลายลักษณ์อักษร	ลูกค้าควรทำสัญญาและข้อตกลงเป็นลายลักษณ์อักษรกับผู้ให้บริการ ซึ่งครอบคลุมถึงขอบเขตของการบริการจ้างทำภายนอก มาตรฐานด้านผลการดำเนินงานและการจัดการความเสี่ยง ข้อตกลงระดับการให้บริการ (SLA) ความต่อเนื่องทางธุรกิจ ค่าบริการ การยุติสัญญาเนื่องจากผิดนัดหรือการถอนตัวล่วงหน้า การแจ้งเหตุการณ์ที่ไม่พึงประสงค์ การรับข้อพิพาท ความเป็นส่วนตัวและความปลอดภัย การจ้างทำภายนอกต่อ การจ้างทำภายนอกต่างประเทศ สิทธิในการตรวจสอบและเนื้อหาอื่นๆ ที่เกี่ยวข้อง Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสองฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ 3-6	การติดตาม ประเมินผล ตรวจสอบ และควบคุมค วามเสี่ยงจาก การใช้บริการ จากผู้ให้บริการ ภายนอก	สถาบันการเงินต้องกำหนดแนวทางกา รบริหารความเสี่ยงที่เกิดจากการใช้บริ การจาก ผู้ให้บริการภายนอกอย่างชัดเจนและ เป็นลายลักษณ์อักษร ให้เหมาะสมกับสำคัญของงานที่ ใช้บริการ จากผู้ให้บริการภายนอก และสอดคล้องกับนโยบายการบริหรค วามเสี่ยงโดยรวม รวมทั้งสื่อสารให้บุคคล ที่เกี่ยวข้องเข้าใจและปฏิบัติตามแนว ทางดังกล่าวอย่างเคร่งครัด โดยต้องพิจารณาให้ครอบคลุมประเดี นสำคัญอย่างน้อยดังต่อไปนี้	ลูกค้าควรจัดทำแนวทางนโยบายการจัดการความเสี่ยง จากการจ้างทำภายนอก ซึ่งควรสอดคล้องกับสำคัญของกิจกรรมการจ้าง ทำภายนอกและนโยบายการจัดการความเสี่ยงโดยรวม ของลูกค้า โดยครอบคลุมหลักๆ ดังนี้: การกำกับดูแลและตรวจสอบผู้ให้บริการเป็นประจำ การกำหนดให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติการและ เอกสารอื่นๆ การฝึกอบรมพนักงานหรือผู้เกี่ยวข้องเพื่อให้เข้าใจขอบ เขตการบริการของผู้ให้บริการ และการบันทึกความเสี่ยงและปัญหาที่เกี่ยวข้องกับการ จ้างทำภายนอก
		(1) จัดให้มีระบบที่ชัดเจนในการกำกับด แล ติดตาม ตรวจสอบ และประเมินผล ผู้ให้บริการภายนอกอย่างเหมาะสม เพื่อให้มีมาตรฐานการควบคุมภายในแ ละการให้บริการเช่นเดียวกับ	Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์ จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประ เทศไทย
		สถาบันการเงินดำเนินการเอง รวมทั้งต้องตรวจสอบให้แน่ใจว่า ทั้งสถาบันการเงินเองและผู้ให้บริการ ภายนอกได้ปฏิบัติตามกฎหมาย มาตรฐานการบัญชี และกฎเกณฑ์ที่เกี่ยวข้องโดยเคร่งครัด	ปัจจุบัน Tencent Cloud ได้รับการรับรองและคุณวุฒิด้านความปลอดภัยและคว ามเป็นส่วนตัวหลายรายการผ่านการตรวจสอบหรือประ เมินโดยบุคคลที่สามที่เป็นอิสระ และตามความต้องการของลูกค้า โดยผ่านการจัดทำรายงานการควบคุมระบบและองค์กร ที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการ ล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคล ที่สามที่เป็นอิสระแล้ว
		(2) จัดให้มีหรือดำเนินการให้ผู้ให้บริการ ภายนอกจัดทำคู่มือการปฏิบัติงานแล ะเอกสาร ที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อประโยชน์ในการติดตาม ประเมินผลและ บริหารความเสี่ยงของสถาบันการเงิน	ขั้นตอนการดำเนินการ คู่มือผู้ใช้ และเอกสารอื่น ๆ ของผลิตภัณฑ์ Tencent Cloud ได้รับการจัดทำเป็นลายลักษณ์อักษรและจัดเตรียมไว้สำ หรับลูกค้าผ่านทางเว็บไซต์อย่างเป็นทางการ นอกจากนี้ Tencent Cloud ยังมอบบริการ Training and Certification
		(3) จัดให้มีพนักงานหรือหน่วยงานที่มีค วามเข้าใจในขอบเขต ลักษณะงานและ กระบวนการทำงานของผู้ให้บริการภา ยนอก เพื่อให้สามารถติดตามและประเมินผล การปฏิบัติงาน ของผู้ให้บริการภายนอกได้อย่างถูกต้ องและน่าเชื่อถือ	

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		(4) จัดให้มีการบันทึกประเด็นปัญหาหรือ ความเสี่ยง ข้อมูลความเสียหาย รวมทั้ง คำสั่งการจากทางการที่เกี่ยวข้องกับก ารให้บริการจากผู้ให้บริการภายนอกเ เพื่อให้ธนาคาร แห่งประเทศไทยตรวจสอบได้ พร้อมทั้งรายงานข้อมูลดังกล่าวต่อผู้บ ริหารของสถาบันการเงิน ให้ทราบในทันที เพื่อให้สามารถกำหนดแนวทางการแก้ ไขปัญหาดังกล่าวได้อย่างเหมาะสมแล ะทันห้วงที่	ที่อ้างอิงจากความรู้ทั่วไปเกี่ยวกับผลิตภัณฑ์ Tencent Cloud และความสามารถทางวิชาชีพที่เกี่ยวข้อง เพื่อเสริมสร้างความสามารถทางเทคนิคและความคล่อง แคล่วในการใช้ระบบคลาวด์ของลูกค้า Tencent Cloud มอบช่องทางหลายช่องทางให้แก่ลูกค้า รวมถึงทีมงาน 24 ชั่วโมงตลอด 7 วัน Hotline 24 ชั่วโมงตลอด 7 วัน บริการลูกค้าอัจฉริยะ บริการตนเอง ฯลฯ เพื่อจัดการปัญหาข้อเสนอนะที่ลูกค้าส่งมาอย่างไม่ชา ดสาย ทีมงานบริการลูกค้าและผู้เชี่ยวชาญด้านเทคนิคของ Tencent Cloud จะมอบการสนับสนุนที่รวดเร็วและมีประสิทธิภาพแก่ลูก ค้า
		(5) จัดให้มีการทบทวนผู้ให้บริการภาย นอกเป็นระยะตามความเหมาะสมของ กลุ่มงาน	

07

Tencent Cloud
จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ
หลักเกณฑ์การให้บริการจาก
พันธมิตรทางธุรกิจ
ของสถาบันการเงิน ของ
BOT อย่างไร

ธนาคารแห่งประเทศไทยได้ออก BOT No. FPG 16/2563 เรื่อง

หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจ (business partner) ของสถาบันการเงิน ในปี 2563

ซึ่งกำหนดให้สถาบันการเงินเมื่อใช้บริการที่ให้โดยพันธมิตรทางธุรกิจ³

ต้องให้ความสำคัญกับความต่อเนื่องทางธุรกิจ การปกป้องลูกค้า

และความรับผิดชอบของตนเองเช่นเดียวกับที่ดำเนินธุรกิจด้วยตนเอง

พร้อมทั้งต้องดำเนินการจัดการความเสี่ยง รับประกันความปลอดภัยของการทำธุรกรรม

และปกป้องข้อมูลลูกค้า ข้อกำหนดหลักครอบคลุมหลักการในการใช้บริการพันธมิตรทางธุรกิจ

ขอบเขตและเงื่อนไขทั่วไปของการใช้บริการพันธมิตรทางธุรกิจ การจัดการความเสี่ยง

และการตรวจสอบโดยธนาคารแห่งประเทศไทย ผู้สอบบัญชีภายนอก หรือหน่วยงานกำกับดูแลอื่นๆ

เป็นต้น

ในบทนี้ Tencent Cloud จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จาก

หลักเกณฑ์การใช้บริการจากพันธมิตรทางธุรกิจ (business partner) ของสถาบันการเงิน

และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud

จะช่วยสถาบันการเงินในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ลูกค้าสามารถใช้บริการของพันธมิตรทางธุรกิจได้ แต่ควรเชื่อมั่นว่าพันธมิตรดังกล่าวมีความสามารถในการ จัดการความเสี่ยงและการปกป้องลูกค้า ลูกค้าควรเชื่อมั่นว่าหน้าที่เชิงกลยุทธ์อยู่ในความรับผิดชอบ ของลูกค้าเอง
5.2.1	หลักการ	สถาบันการเงินสามารถใช้บริการจาก พันธมิตรทางธุรกิจทั้งที่เป็นนิติบุคคล และบุคคลธรรมดา โดยต้องมีแนวทางการบริหารความเสี ยและแนวทางการดูแลผู้ใช้บริการที่ เหมาะสมได้ยกเว้นงานหลักที่เกี่ยวข้อง กับการตัดสินใจเชิงกลยุทธ์ (strategic function) สถาบัน การเงินยังต้องดำเนินการด้วยตนเอง	การจัดการความเสี่ยง Tencent Cloud ได้กำหนดกรอบการกำกับดูแลความเสี่ยงและขั้นตอนที่ เกี่ยวข้อง และปรับปรุงมาตรการจัดการความเสี่ยงและระบบตรวจ สอบภายในอย่างต่อเนื่อง โดยการเสริมสร้างวัฒนธรรมความเสี่ยงอย่างต่อเนื่อง Tencent Cloud ปรับปรุงความสามารถในการจัดการความเสี่ยงภายใน อย่างมีประสิทธิภาพ และรับประกันการพัฒนาทางธุรกิจที่ยั่งยืนและมีสุขภาพ ดี ในด้านการปกป้องลูกค้า Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจ ศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด Tencent Cloud

³ พันธมิตรทางธุรกิจ: (1) การแต่งตั้งตัวแทนทางการเงิน (banking agent) การใช้ผู้ให้บริการภายนอก (outsourcing) และการร่วมมือกับพันธมิตรทางธุรกิจในรูปแบบอื่น

ให้ถือว่าเป็นการใช้บริการจากพันธมิตรทางธุรกิจ (business partner)

(2) สถาบันการเงินสามารถใช้บริการจากพันธมิตรทางธุรกิจทั้งที่เป็นนิติบุคคลและ บุคคลธรรมดา

เพื่อสนับสนุนการดำเนินธุรกิจของสถาบันการเงินได้

(3) กรณีพันธมิตรทางธุรกิจในรูปแบบตัวแทนทางการเงินที่ต้องมีสถานที่ในการให้บริการ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ได้สร้างกรอบการปกป้องความเป็นส่วนตัวที่เน้นผู้ใช้เป็นศูนย์กลางภายในองค์กร โดยผ่านกระบวนการและเครื่องมือประเมินการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวที่สมบูรณ์ พร้อมทั้งผสมผสานมาตรฐานสากล นวัตกรรมทางเทคโนโลยี และการฝึกอบรมพนักงาน ทำให้การปกป้องความเป็นส่วนตัวกลายเป็นส่วนหนึ่งของหลายด้านในการสร้างวัฒนธรรมองค์กร เพื่อให้แน่ใจว่าความเป็นส่วนตัวของลูกค้าได้รับการปกป้องอย่างเคร่งครัดสูงสุด
5.3.1 (3)	พันธมิตรทางธุรกิจภายในและภายนอกประเทศ	(3)สถาบันการเงินสามารถใช้บริการจากพันธมิตรทางธุรกิจที่เป็นนิติบุคคลหรือบุคคลธรรมดา ทั้งที่อยู่ในประเทศและต่างประเทศ	ลูกค้าสามารถเลือกใช้บริการจากพันธมิตรทางธุรกิจที่ตั้งอยู่ในประเทศไทยหรือนอกประเทศได้ โครงสร้างพื้นฐานของ Tencent Cloud ครอบคลุมหลายพื้นที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) โดยแต่ละภูมิภาคเป็นพื้นที่ทางภูมิศาสตร์ที่แยกอิสระ และแต่ละโซนความพร้อมใช้งานเป็นโดเมนการบำรุงรักษาและรับมือเหตุขัดข้องที่แยกจากกัน โซนความพร้อมใช้งานแต่ละแห่งถูกแยกทางกายภาพ ลูกค้าสามารถวางระบบและจัดเก็บข้อมูลบนภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระตามความต้องการในการขยายธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อรับประกันความต้องการด้านการรับมือเหตุขัดข้องของธุรกิจ ภายในปี 2026 Tencent Cloud ได้ดำเนินการติดตั้งศูนย์ข้อมูลสามแห่งในประเทศไทย โดยศูนย์ข้อมูลแต่ละแห่งมีการจัดการด้านไฟฟ้าและเครือข่ายที่เป็นอิสระต่อกัน เพื่อรองรับการจัดเก็บประมวลผล และสำรองข้อมูลของลูกค้าภายในประเทศได้อย่างมีประสิทธิภาพ
5.3.3 (2)	หลักการสำคัญ	(2)สถาบันการเงินยังคงต้องดูแลให้พันธมิตรทางธุรกิจสามารถให้บริการแก่ผู้ใช้บริการเสมือนสถาบันการเงินเป็นผู้ดำเนินการเอง โดยยึดหลักการสำคัญ 3 ประการ ได้แก่ 1) การดูแล สิทธิขั้นพื้นฐานของผู้ใช้บริการอย่างเหมาะสม	ลูกค้าควรให้มั่นใจในคุณภาพการบริการที่พันธมิตรทางธุรกิจจัดหาให้ และควรกำหนดให้พันธมิตรทางธุรกิจของตนจัดเตรียมการปกป้องที่เหมาะสมสำหรับความปลอดภัยของข้อมูลลูกค้า การจัดการข้อร้องเรียนของลูกค้า และปัญหาเกี่ยวกับบริการ ให้ความรับประกันความต่อเนื่องทางธุรกิจ และสร้างระบบการจัดการความเสี่ยง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		โดยเฉพาะการรักษาความปลอดภัยของข้อมูล การร้องเรียน และแก้ปัญหา 2)ความต่อเนื่องในการดำเนินงานธุรกิจและ 3)การมีระบบบริหารความเสี่ยงจากกาใช้บริการ อย่างเหมาะสมตามระดับความมีนัยสำคัญและผลกระทบ ครอบคลุมความเสี่ยงที่เกี่ยวข้อง โดยเฉพาะ ความเสี่ยงด้านชื่อเสียงด้านปฏิบัติการ และด้านเทคโนโลยีสารสนเทศ โดยมีแนวทางการคัดเลือก พันธมิตรทางธุรกิจและการบริหารจัดการความเสี่ยงในการใช้บริการจากพันธมิตรทางธุรกิจที่ครอบคลุม ประเด็นสำคัญ	ในด้านการจัดการความปลอดภัยของข้อมูลลูกค้า การจัดการข้อร้องเรียนของลูกค้า และการแก้ไขปัญหาบริการ ข้อมูลของลูกค้าภายใน Tencent Cloud จัดอยู่ในระดับความปลอดภัยสูงสำหรับพนักงานภายใน Tencent Cloud หากไม่ใช้บริการที่ลูกค้าเลือกใช้ซึ่งจำเป็นต้องประมวลผลข้อมูลของลูกค้า พนักงาน Tencent Cloud จะไม่พยายามเข้าถึงข้อมูลลูกค้าใดๆ Tencent Cloud ใช้ระบบตรวจสอบและบำรุงรักษาการยืนยันตัวตนด้วยชื่อจริงแบบเต็มทุกขั้นตอนสำหรับสิทธิ์การเข้าถึงข้อมูลเพื่อรับประกันความสมบูรณ์ของสินทรัพย์ข้อมูลและความน่าเชื่อถือของบริการธุรกิจ และได้สร้างกลไกการตรวจสอบและล็อกแบบเรียลไทม์เพื่อตรวจจับและป้องกันพฤติกรรมการณ์การเข้าถึงข้อมูลที่ผิดปกติใดๆ Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสองฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้ นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้าได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเวล ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับการสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า ในด้านการรับประกันความต่อเนื่องทางธุรกิจ Tencent Cloud ได้ออกแบบและนำกรอบการจัดการความต่อเนื่องของธุรกิจที่เหมาะสมกับสภาพแวดล้อมคอมพิวเตอร์คลาวด์ของตนเองไปใช้ สร้างระบบการจัดการความต่อเนื่องของธุรกิจที่ครอบคลุม และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจแล้ว จัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดยละเอียดสำหรับผลิตภัณฑ์คลาวด์และกระบวนการสำคัญ Tencent Cloud จะทำการทดสอบฝึกซ้อมความต่อเนื่องของธุรกิจสำหรับผลิตภัณฑ์คลาวด์เป็นประจำตามแผนความต่อเนื่องของธุรกิจ เพื่อให้แน่ใจในความสามารถในการปฏิบัติได้จริงของแผน แผนฉุกเฉิน ฯลฯ ในด้านระบบการจัดการความเสี่ยง Tencent Cloud ได้สร้างกรอบการจัดการความเสี่ยงที่ครอบคลุมตามมาตรฐาน ISO/IEC 27001:2022 และดำเนินการประเมินความเสี่ยงอย่างน้อยปีละหนึ่งครั้ง โดยระบุความเสี่ยงตามผลการวิเคราะห์กระบวนการของสถานการณ์ความเสี่ยง ผลิตภัณฑ์หรือบริการทางธุรกิจ สำหรับความเสี่ยงที่ระบุ Tencent Cloud จะประเมินความเป็นไปได้และระดับผลกระทบของความเสี่ยงแต่ละรายการ จำแนกระดับความเสี่ยง ดำเนินการตามขั้นตอนที่สอดคล้องกันต่อไป และบันทึกไว้เป็นหลักฐาน Tencent Cloud ยังติดตามสถานการณ์การจัดการความเสี่ยงอย่างต่อเนื่อง ประเมินความเสี่ยงที่เหลืออยู่ และให้มั่นใจว่าผู้เกี่ยวข้องได้จัดการความเสี่ยงอย่างเหมาะสมตามข้อกำหนดการจัดการความเสี่ยงของ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
5.3.3 (3)	การปฏิบัติ ตามกฎหมายและ ระเบียบข้อบ งคับ	(3)สถาบันการเงินต้องดูแลให้พันธมิตรทางธุรกิจที่ด เนินการแทนสถาบันการเงิน ปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน กฎหมายว่าด้วยการควบคุมการแลกเปลี่ยนเงิน และประกาศธนาคารแห่งประเทศไทยว่าด้วยการบริหารจัดการด้านการให้บริการแก่ลูกค้าอย่าง เป็นธรรม (Market conduct)	ลูกค้าควรให้มั่นใจว่าพันธมิตรทางธุรกิจปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องในท้องถิ่นของประเทศไทย Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด ปัจจุบัน Tencent Cloud ได้รับการรับรองและคุณสมบัติด้านความปลอดภัยและความเป็นส่วนตัวหลายรายการผ่านการตรวจสอบหรือประเมินโดยบุคคลที่สามที่เป็นอิสระ และตามความต้องการของลูกค้า โดยผ่านการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจาก " Compliance Document Download "
		(4)สถาบันการเงินต้องดูแลให้ผู้รับจ้าง ช่วง (subcontract) จากพันธมิตร ทางธุรกิจทุกทอดปฏิบัติตามหลักเกณฑ์และเงื่อนไขที่ก	ลูกค้าควรให้มั่นใจว่าพันธมิตรทางธุรกิจจัดการผู้รับช่วงงานของตน Tencent Cloud ได้จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement สำหรับสถานการณ์การประมวลผลโดยผู้รับช่วงงาน ข้อตกลงได้กำหนดข้อกำหนดต่างๆ อย่างชัดเจน เช่น การให้ความยินยอมล่วงหน้าสำหรับการรับช่วงงาน การแจ้งเตือนก่อนการเพิ่มหรือเปลี่ยนผู้รับช่วงงาน หน้าที่ในการปกป้องข้อมูล เป็นต้น โดยปราศจากความยินยอมล่วงหน้าจากลูกค้า Tencent Cloud จะไม่รับช่วงงานการดำเนินการประมวลผลใดๆ ที่ดำเนินการแทนลูกค้าตามสัญญา/ข้อตกลง การเปลี่ยนแปลงใดๆ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ที่คาดว่าจะเพิ่มหรือเปลี่ยนแปลงผู้รับช่วงงาน Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านช่องทางต่างๆ เช่น อีเมล นอกจากนี้ ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้ ในด้านการจัดการผู้รับช่วงงาน Tencent Cloud ได้สร้างระบบการจัดการความปลอดภัยทางโซลูชันที่สมบูรณ์ โดยผ่านมาตรการต่างๆ เช่น การประเมินและตรวจสอบการอนุญาตเข้าความปลอดภัยของผู้จัดหาที่เข้มงวด การตรวจสอบและประเมินเป็นประจำ และข้อตกลงการบริการรับช่วงงานที่ชัดเจน เพื่อควบคุมผู้จัดหาได้อย่างมีประสิทธิภาพ และรับประกันว่าการรับช่วงงานจะไม่ส่งผลกระทบต่อความสามารถของ Tencent Cloud ในการให้บริการที่เกี่ยวข้องแก่ลูกค้า ความเป็นความลับและความสมบูรณ์ของกระบวนการประมวลผลข้อมูลลูกค้า ตลอดจนสิทธิในการกำกับดูแลและตรวจสอบของหน่วยงานกำกับดูแลทางการเงินและสถาบันการเงินของประเทศไทย นอกจากนี้ Tencent Cloud จะให้ความร่วมมืออย่างแข็งขันกับข้อกำหนดการจัดการรับช่วงงานของลูกค้า ตอบสนองและสนับสนุนกิจกรรมการตรวจสอบหรือการประเมินที่ลูกค้าเป็นผู้ริเริ่ม เป็นต้น
5.5	การตรวจสอบโดยธนาคารแห่งประเทศไทย	การตรวจสอบโดยธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือหน่วยงาน กำกับดูแลอื่น สถาบันการเงินต้องดำเนินการให้ธนาคารแห่งประเทศไทย ผู้ตรวจสอบภายนอก หรือ หน่วยงานของทางการอื่นสามารถเข้าตรวจสอบพันธมิตรทางธุรกิจที่ดำเนินการแทนสถาบันการเงิน หรือผู้รับจ้างช่วง (ถ้ามี) ได้ รวมทั้งจัดเตรียมข้อมูลที่เกี่ยวข้องกับงานที่ใช้บริการให้มีความถูกต้องและเป็นปัจจุบันไว้ให้ตรวจสอบได้ด้วย	ลูกค้าควรให้มั่นใจว่าธนาคารแห่งประเทศไทย ผู้สอบบัญชีภายนอก หรือหน่วยงานกำกับดูแลอื่นๆ สามารถดำเนินการตรวจสอบพันธมิตรทางธุรกิจและผู้รับช่วงงานของตนได้ Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเทศไทย ปัจจุบัน Tencent Cloud ได้รับการรับรองและคุณวุฒิด้านความปลอดภัยและความเป็นส่วนตัวหลายรายการผ่านการตรวจสอบหรือประเมินโดยบุคคลที่สามที่เป็นอิสระ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และตามความต้องการของลูกค้า โดยผ่านการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจาก " Compliance Document Download"
เอกสารแนบ 3	แนวทางการคัดเลือกพันธมิตรทางธุรกิจ	สถาบันการเงินจะต้องกำหนดแนวทางการคัดเลือกพันธมิตรทางธุรกิจอย่างเหมาะสมก่อนการทาสัญญาหรือข้อตกลงร่วมกันหรือทบทวนเพื่อต่ออายุสัญญาหรือข้อตกลงนั้นโดยสถาบันการเงินต้องกำหนดแนวทางการคัดเลือกพันธมิตรทางธุรกิจตามระดับความเสี่ยงและการใช้บริการโดยครอบคลุมประเด็นสำคัญดังต่อไปนี้ (1)ความสามารถทางเทคนิค ความเชี่ยวชาญประสบการณ์ในการดำเนินงาน และความพร้อมในการให้บริการ (2)สถานะความมั่นคงทางการเงิน (3)ชื่อเสียงทางธุรกิจ ประวัติการถูกร้องเรียน หรือถูกฟ้องร้องดำเนินคดี (4)วัฒนธรรมองค์กรและนโยบายการให้บริการที่มีความเหมาะสมกับสถาบันการเงิน (5)ความสามารถในการปรับตัวตอบสนองต่อการพัฒนาการใหม่ ๆ (6)ความเสี่ยงในกรณีที่พันธมิตรทางธุรกิจ	ลูกค้าควรกำหนดเกณฑ์ในการเลือกผู้ให้บริการให้ชัดเจนก่อนการลงนามในสัญญาใหม่หรือต่ออายุสัญญา โดยครอบคลุมประเด็นหลักดังต่อไปนี้: ความสามารถทางเทคนิคและความเชี่ยวชาญ ความมั่นคงทางการเงิน ชื่อเสียงทางธุรกิจ วัฒนธรรมองค์กรที่สอดคล้องกับสถาบันการเงิน ความสามารถในการปรับตัวต่อการพัฒนาการใหม่ ๆ ความเสี่ยงด้านความเข้มข้น (concentration risk) รวมถึงข้อกำหนดที่ชัดเจนเกี่ยวกับการมอบหมายงานด้านที่เกี่ยวข้องกับคณะกรรมการและผู้บริหารระดับสูงให้กับผู้ให้บริการภายนอก Tencent Cloud ได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบอย่างละเอียดของลูกค้าอย่างเข้มข้น ต่อไปนี้เป็นภาพรวมของ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ในด้านต่างๆ ของการตรวจสอบอย่างละเอียด: • ความสามารถทางวิชาชีพและทางเทคนิค : Tencent Cloud ได้แสดงความสามารถทางเทคนิคที่ครอบคลุมในฐานะผู้นำในอุตสาหกรรมผ่านเทคโนโลยีคอมพิวเตอร์คลาวด์ที่แข็งแกร่ง ความสามารถในการประมวลผลข้อมูลขนาดใหญ่ การประยุกต์ใช้ปัญญาประดิษฐ์ การป้องกันความปลอดภัยทางไซเบอร์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
	ธุรกิจ ให้บริการแก่สถาบันการเงินอื่นหรือผู้ นหลายแห่ง พร้อมกัน (concentration risk) (7)มีหลักเกณฑ์ในการพิจารณาการ ให้บริการจากพันธมิตรทางธุรกิจ ที่มีส่วนเกี่ยวข้อง คณะกรรมการและผู้บริหารระดับสูง (conflict of interest)	เทคโนโลยีคลาวด์ในทีฟ การกระจายตัวของศูนย์ข้อมูลทั่วโลก และโซลูชันอุตสาหกรรม ความสามารถทางเทคนิคเหล่านี้ไม่เพียงรับประกันความ มั่นคงและความน่าเชื่อถือของบริการ Tencent Cloud เท่านั้น แต่ยังจัดเตรียมสภาพแวดล้อมคอมพิวเตอร์คลาวด์ที่ปล อดภัยและน่าเชื่อถือให้กับลูกค้าด้วย ความสามารถด้านความปลอดภัยในการดำเนินงานที่ค รบกวันของ Tencent Cloud ยังสามารถให้การสนับสนุนทางเทคนิครอบนาฬิกาสำหรับ รับผลิตภัณฑ์คลาวด์แก่ลูกค้าได้	• ประสบการณ์ในการดำเนินงาน: ความสามารถในการดำเนินงานและขนาดของ Tencent Cloud อยู่ในตำแหน่งผู้นำในอุตสาหกรรม ศูนย์ข้อมูลของ Tencent Cloud มีการกระจายตัวอยู่ในหลายภูมิภาคทั่วโลก ครอบคลุมพื้นที่จีนแผ่นดินใหญ่ ภูมิภาคเอเชียแปซิฟิก ภูมิภาคอเมริกาเหนือ และภูมิภาคยุโรป • สภาพทางการเงิน: Tencent Cloud ซึ่งเป็นแบรนด์คอมพิวเตอร์คลาวด์ที่ Tencent Group สร้างขึ้นด้วยความอุตสาหกรรม ได้รับประโยชน์จากความแข็งแกร่งทางการเงินและสภ พทางการเงินที่มั่นคงของ Tencent Group นับตั้งแต่ปี 2010 ที่ Tencent Cloud เริ่มให้บริการคลาวด์แก่สาธารณะอย่างเป็นทางการ Tencent Cloud ได้บรรลุแนวโน้มการเติบโตที่โดดเด่นในตัวชี้วัดทางกา รเงินที่สำคัญ เช่น รายได้และผลกำไร Tencent Cloud ได้รับการยอมรับจากสถาบันวิจัยอุตสาหกรรมระดับโลก ชั้นนำ Gartner ติดต่อกันเป็นเวลาสี่ปี โดยอยู่ในอันดับที่สองในด้านมิติด้านกลยุทธ์ในหมวดผู้ ผลิตจากประเทศจีน • ชื่อเสียงทางธุรกิจ: ในฐานะแบรนด์คอมพิวเตอร์คลาวด์ภายใต้การนำของ Tencent ซึ่งเป็นบริษัทชั้นนำในอุตสาหกรรมอินเทอร์เน็ตของจีน Tencent Cloud ได้รับการรับรองจากสถาบันอุตสาหกรรมหลายแห่ง มอบโซลูชันคอมพิวเตอร์คลาวด์ที่ครอบคลุม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และได้ร่วมมือกับพันธมิตรมากกว่า 11,000 ราย เพื่อมอบโซลูชันอุตสาหกรรมมากกว่า 400 รายการให้กับลูกค้าธุรกิจในกว่า 30 อุตสาหกรรม วัฒนธรรมองค์กรและนโยบายการให้บริการ ที่มีความเหมาะสมกับสถาบันการเงิน: Tencent Cloud สามารถปรับโซลูชันให้เหมาะสมตามความต้องการของ ลูกค้า ปรับตัวได้อย่างยืดหยุ่นกับวัฒนธรรมและกลยุทธ์ขององ ค์กรที่แตกต่างกัน Tencent Cloud ได้ปรับแต่งโซลูชันต่างๆ ให้เหมาะสมสำหรับสถาบันการเงินหลายแห่ง มอบบริการคลาวด์เฉพาะสำหรับการเงินที่สอดคล้องกับ ข้อกำหนดด้านกฎระเบียบให้กับลูกค้าทางการเงินหลา ยราย และมีขีดความสามารถในการปฏิบัติตามข้อกำหนดด้าน ความปลอดภัยระดับการเงิน ความสามารถในการปรับตัวต่อพัฒนาการ ใหม่: Tencent Cloud ติดตามแนวโน้มตลาดและการพัฒนาทางเทคโนโลยีย างแข่งขัน ออกผลิตภัณฑ์และบริการใหม่ อย่างต่อเนื่อง เพื่อรักษาตำแหน่งผู้นำในตลาดและตอบสนองความต้อ งการล่าสุดของลูกค้า การจัดการความเสี่ยง: Tencent Cloud ได้กำหนดกรอบการกำกับดูแลความเสี่ยงและขั้นตอนที่ เกี่ยวข้อง และปรับปรุงมาตรการจัดการความเสี่ยงและระบบตรวจ สอบภายในอย่างต่อเนื่อง โดยการเสริมสร้างวัฒนธรรมความเสี่ยงอย่างต่อเนื่อง Tencent Cloud ปรับปรุงความสามารถในการจัดการความเสี่ยงภายในอ ย่างมีประสิทธิภาพ และรับประกันการพัฒนาทางธุรกิจที่ยั่งยืนและมีสุขภาพ ดี

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
เอกสารแนบ 4	ประเด็นที่ควร ครอบคลุมใน สัญญาหรือข้อ ตกลงกับพันธมิตรทางธุรกิจ	สถาบันการเงินต้องท าสัญญาหรือข้อตกลงกับพันธมิตรทาง ธุรกิจที่จะใช้บริการเป็นลายลักษณ์อ ักษร	ลูกค้าควรทำสัญญาและข้อตกลงเป็นลายลักษณ์อักษร กับผู้ให้บริการ ซึ่งครอบคลุมถึงขอบเขตของการบริการจ้างทำภายนอก มาตรฐานด้านผลการดำเนินงานและการจัดการความเสี่ยง ข้อตกลงระดับการให้บริการ (SLA) ความต่อเนื่องทางธุรกิจ ค่าบริการ การยุติสัญญาเนื่องจากผิดนัดหรือการถอนตัวล่วงหน้า การแจ้งเหตุการณ์ที่ไม่พึงประสงค์ การรับข้อพิพาท ความเป็นส่วนตัวและความปลอดภัย การจ้างทำภายนอกต่อ การจ้างทำภายนอกต่างประเทศ สิทธิในการตรวจสอบ และเนื้อหาอื่นๆ ที่เกี่ยวข้อง
			Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็น ทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งส องฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้

08

Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ

เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ตามกฎหมายว่าด้วยระบบการชำระเงิน ของ BOT อย่างไร

ธนาคารแห่งประเทศไทยได้จัดทำ BOT No. SorNorChor 1/2564

เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk)
ตามกฎหมายว่าด้วยระบบการชำระเงิน

บนพื้นฐานของกรอบการกำกับดูแลเทคโนโลยีสารสนเทศที่มีอยู่ในปัจจุบัน

โดยมีวัตถุประสงค์เพื่อให้แน่ใจว่าระบบการชำระเงินและผู้ให้บริการที่อยู่ภายใต้การกำกับดูแลมีระบบการกำกับดูแลเทคโนโลยีสารสนเทศที่ดี รับประกันความปลอดภัยด้านเทคโนโลยีสารสนเทศ และจัดการความเสี่ยงที่เกี่ยวข้องอย่างเหมาะสม

ข้อกำหนดด้านการกำกับดูแลการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศของกฎเกณฑ์การกำกับดูแลนี้ประกอบด้วยสองส่วนหลัก:

- การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene):
นี่คือมาตรการความปลอดภัยพื้นฐานที่ระบบการชำระเงินและผู้ให้บริการทั้งหมดที่อยู่ภายใต้การกำกับดูแลต้องปฏิบัติตาม
โดยมีวัตถุประสงค์เพื่อยกระดับระดับการป้องกันความปลอดภัยและความยืดหยุ่นในการป้องกันและรับมือกับภัยคุกคามทางเครือข่ายที่สำคัญ
- การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management): ใช้กับระบบการชำระเงินที่มีความสำคัญ⁴ และผู้ให้บริการของระบบดังกล่าว
โดยกำหนดให้ต้องมีกรอบการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม ซึ่งรวมถึงการมีโครงสร้างองค์กรและองค์ประกอบการจัดการที่เหมาะสม
ตลอดจนบทบาทหน้าที่ที่ชัดเจนของคณะกรรมการในการกำหนดนโยบายการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุม และการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
เพื่อให้สอดคล้องกับลักษณะของการให้บริการหรือการดำเนินงานทางธุรกิจ
ข้อกำหนดของภาคผนวกและแนบบริคมีเนื้อหาหลักที่สอดคล้องเป็นอย่างยิ่งกับภาคผนวกและแนบบริคของกฎหมาย หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
แต่ในด้านข้อกำหนดการควบคุมนั้นมีลักษณะที่เรียบง่ายกว่ากฎเกณฑ์ดังกล่าว
ในฐานะผู้ให้บริการคลาวด์ วิธีการที่ Tencent Cloud
ปฏิบัติตามและช่วยเหลือลูกค้าให้เป็นไปตามข้อกำหนดที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ สถาบันการเงินสามารถอ้างอิงเนื้อหาในขอบเขตที่เกี่ยวข้องของบทที่ 5
Tencent Cloud จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ
หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ของ BOT อย่างไร ในเอกสารนี้ตามความเหมาะสม

ในบทที่ Tencent Cloud จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จากเรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ

⁴ ระบบการชำระเงินที่มีความสำคัญ: (1) ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ

(2) ผู้ประกอบธุรกิจระบบการชำระเงินภายใต้การกำกับ

(3) ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับที่มีคุณสมบัติ ดังต่อไปนี้

(3.1) เชื่อมต่อโดยตรงกับระบบการชำระเงินภายใต้การกำกับ หรือเชื่อมต่อกับ ผู้ให้บริการแก่ผู้รับบัตร (acquirer)

หรือเชื่อมต่อกับธนาคารที่ให้บริการเชื่อมต่อระบบ (sponsor bank)

(3.2) ให้บริการทางการเงินแก่ลูกค้าผ่านเครือข่ายสื่อสารสาธารณะ (Internet facing)

(3.3) มีบัญชีผู้ใช้งานมากกว่า 5 ล้านบัญชี หรือมีปริมาณธุรกรรมมากกว่า 10 ล้านรายการต่อปี

ตามกฎหมายว่าด้วยระบบการชำระเงิน และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud จะช่วยสถาบันการเงินในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

8.1 การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
5.1.1	การก หนดมาตรฐาน ด้านการรั กษาความม ั่นคงปลอดภัย ของระบบ เทคโนโลยีสร สนเทศ	กำหนดมาตรฐานการรักษาความม ั่นคงปลอดภัยขั้นต่ำ(minimum security baseline) และตั้งค่าการรักษาความมั่นคงปลอ ดภัยสอดคล้องกับการให้บริการ (security hardening) ให้ครอบคลุมระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล(database system) ระบบงาน (application) อุปกรณ์เครือข่ายและอุปกรณ์รักษา ความปลอดภัยเครือข่ายที่รองรับระ บบงานสำคัญให้ชัดเจนเป็นลายลัก ษณ้อักษร รวมทั้งดำเนินการและสอบทานตาม ที่ได้ก ำหนดไว้ หากมีเหตุผู้ให้บริการและผู้ประก อบธุรกิจไม่สามารถปฏิบัติตามมาตรฐ าน ที่กำหนดไว้ต้องจัดให้มีกระบวนการ ขออนุมัติยกเว้น(exception) เพื่อประเมินความเสี่ยงและพิจารณา แนวทางควบคุมความเสี่ยงที่เพียงพอ เหมาะสมก่อนด ำเนินการ	ลูกค้าควรกำหนดเส้นฐานความปลอดภัย (security baseline) สำหรับระบบที่สำคัญ และทบทวนและตรวจสอบความถูกต้องและความทันเวลา ของข้อมูลการกำหนดค่าเป็นประจำ หากลูกค้าไม่สามารถปฏิบัติตามเส้นฐานการกำหนดค่า นั้นได้ ควรดำเนินการประเมินความเสี่ยงและใช้มาตรการควบคุม ที่เหมาะสมเพื่อจัดการความเสี่ยง ลูกค้าสามารถใช้บริการ Cloud Workload Protection Platform (CWPP) ซึ่งอิงตามข้อมูลภัยคุกคามจำนวนมหาศาลที่ Tencent รวบรวมสะสมมา สามารถช่วยลูกค้าจัดการความปลอดภัยของเส้นฐานได้ CWPP รองรับการตรวจจับเส้นฐาน รวมถึงโหมดต่างๆ ที่สามารถเลือกได้ เช่น การตรวจจับด้วยคลิกเดียวและการตรวจจับเป็นประจำ และรองรับการดูอัตราการผ่านเส้นฐานและคำแนะนำในก ารแก้ไข CWPP ยังจัดเตรียมนโยบายเส้นฐานเริ่มต้นของ Tencent Cloud ซึ่งช่วยให้ลูกค้าจัดการความปลอดภัยเส้นฐานของเซิร์ฟ เวอร์ได้ดียิ่งขึ้น Cloud Security Center (CSC) ให้ฟังก์ชันการตรวจสอบและประเมินความเสี่ยงการกำหนด ค่าผลิตภัณฑ์คลาวด์โดยอัตโนมัติ ช่วยลูกค้าลดความเสี่ยงด้านความปลอดภัยที่เกิดจากข้อ ผิดพลาดในการกำหนดค่าความปลอดภัยในการใช้ผลิตภัณฑ์ คลาวด์ และยกระดับความปลอดภัยโดยรวมบนคลาวด์ ในเวลาเดียวกัน ลูกค้าสามารถใช้ Config เพื่อดำเนินการตรวจสอบและควบคุมทรัพยากรคลาวด์จา กส่วนกลาง บันทึกข้อมูลการกำหนดค่าและการเปลี่ยนแปลงการกำหนด ค่าของทรัพยากรคลาวด์ต่างๆ ในภูมิภาคต่างๆ ภายใต้บัญชีของลูกค้าอย่างต่อเนื่อง และอิงตามกฎข้อปฏิบัติที่ดีที่สุดและเทมเพลตแพ็คเกจการ ปฏิบัติตามข้อกำหนดของ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อประเมินความสอดคล้องของการกำหนดค่าทรัพยากรคลาวด์ภายใต้บัญชีองค์กรอย่างต่อเนื่องโดยอัตโนมัติ และระบุการกำหนดค่าทรัพยากรที่ไม่สอดคล้อง เพื่อให้บรรลุการตรวจสอบและจัดการทรัพยากรคลาวด์โดยอัตโนมัติ เพื่อให้สอดคล้องกับข้อกำหนดการกำกับดูแลของลูกค้า Tencent Cloud ได้กำหนดมาตรฐานการกำหนดค่าความปลอดภัยเครือข่ายและมาตรฐานเส้นฐานความปลอดภัยขั้น เพื่อจัดการมาตรฐานการกำหนดค่าความปลอดภัยของอุปกรณ์เครือข่าย ไฟร์วอลล์ ระบบปฏิบัติการของเซิร์ฟเวอร์โฮสต์ ฐานข้อมูล และระบบแอปพลิเคชัน Tencent Cloud ใช้เครื่องมือสแกนเพื่อตรวจจับความเบี่ยงเบนของการกำหนดค่าระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และอิมเมจเสมือน (Virtual Image) จากมาตรฐานอย่างต่อเนื่อง สำหรับความเบี่ยงเบนที่ตรวจพบ Tencent Cloud จะสร้างใบงานความปลอดภัยและส่งไปยังทีมงานผู้รับผิดชอบโดยอัตโนมัติ เพื่อดำเนินการแก้ไขทันทีที่ Tencent Cloud ยังทบทวนนโยบายความปลอดภัยและการตั้งค่าพารามิเตอร์ของอุปกรณ์เครือข่าย เช่น เราเตอร์ ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย เป็นระยะ เพื่อให้มั่นใจในประสิทธิภาพของนโยบายและพารามิเตอร์
5.1.2	การป้องกันภัยจากโปรแกรมไม่ประสงค์	จัดให้มีเครื่องมือสำหรับป้องกันภัยจาก malware รวมทั้งติดตามให้มีการ ปรับปรุงให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตีโดย malware	ลูกค้าควรปรับใช้เครื่องมือป้องกันโปรแกรมที่เป็นอันตราย และอัปเดตฐานข้อมูลไวรัสอย่างทันเวลาที่ เพื่อรับมือกับภัยคุกคามที่เกิดขึ้นใหม่ ลูกค้าสามารถใช้ Cloud Workload Protection Platform (CWPP) ใช้ข้อมูลภัยคุกคามจำนวนมากมหาศาลที่รวบรวมสะสมมา โดยใช้การเรียนรู้ของเครื่อง (Machine Learning) เพื่อให้บริการป้องกันความปลอดภัยแก่ลูกค้า เช่น การตรวจจับการบุกรุกของแฮกเกอร์ การแจ้งเตือนความเสี่ยงจากช่องโหว่ รวมถึงฟังก์ชันความปลอดภัยต่าง ๆ เช่น การบล็อกการถอดรหัสสแปม การแจ้งเตือนการเข้าสู่ระบบที่ผิดปกติ การตรวจจับไฟล์มัลแวร์โทรจัน การตรวจจับช่องโหว่ที่มีความเสี่ยงสูง เพื่อแก้ไขความเสี่ยงด้านความปลอดภัยเครือข่ายหลักที่

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เซิร์ฟเวอร์กำลังเผชิญอยู่ในปัจจุบัน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการป้องกันอุปกรณ์ปลายทางของโฮสต์ Tencent Cloud ได้ปรับใช้เครื่องมือตรวจจับและตอบสนองจุดปลายทาง (EDR) เพื่อตรวจสอบและควบคุมสินทรัพย์อุปกรณ์ปลายทางของเซิร์ฟเวอร์ทั่วทั้งเครือข่ายอย่างครอบคลุม เครื่องมือ EDR ที่ Tencent Cloud ใช้สนับสนุนการป้องกันไวรัสและการตรวจจับการบุกรุก เส้นฐานความปลอดภัยและการสแกนช่องโหว่ รวมถึงการตรวจสอบความสอดคล้องด้านความปลอดภัยสำหรับการดำเนินการคำสั่งและพฤติกรรมการเข้าสู่ระบบ และจะทริกเกอร์การแจ้งเตือนเมื่อตรวจพบโปรแกรมที่เป็นอันตรายหรือพฤติกรรมที่ผิดปกติ Tencent Cloud ติดตามและจัดการเหตุการณ์แจ้งเตือนผ่านระบบไปงาน
5.1.3	การบริหารจัดการ security patch	จัดให้มีกระบวนการบริหารจัดการ security patch สำหรับทุกระบบงาน และอุปกรณ์เพื่อเป็นการลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศถูกโจมตีจากช่องโหว่ใหม่ๆ โดยต้องดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่และระดับ ความสำคัญของระบบงาน หากมีเหตุที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ๆ ที่เพิ่งค้นพบ ผู้ให้บริการและผู้ประกอบธุรกิจต้องจัดให้มีการควบคุมอื่นทดแทนเพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้นๆ อย่างไรก็ตาม กรณีที่ไม่สามารถติดตั้ง security patch ได้ต้องจัดให้มี กระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยงรวมทั้งพิ	ลูกค้าควรสร้างขั้นตอนการจัดการแพตช์ความปลอดภัยและดำเนินการติดตั้งแพตช์ตามความรุนแรงของแพตช์และความสำคัญของระบบ หากยังไม่มีแพตช์ความปลอดภัยอย่างเป็นทางการสำหรับช่องโหว่ที่ค้นพบใหม่หรือไม่สามารถติดตั้งแพตช์ความปลอดภัยได้ ลูกค้าควรใช้มาตรการควบคุมที่เหมาะสมเพื่อจัดการความเสี่ยง ลูกค้ายังสามารถใช้ Cloud Workload Protection Platform (CWPP) เพื่อตรวจจับช่องโหว่ซอฟต์แวร์ Linux ช่องโหว่ระบบปฏิบัติการ Windows ช่องโหว่ Web-CMS และช่องโหว่แอปพลิเคชัน แจ้งเตือนแบบเรียลไทม์ และรับโซลูชันการแก้ไขช่องโหว่ ช่วยลูกค้าตอบสนองต่อความเสี่ยงจากช่องโหว่อย่างรวดเร็ว หรือ Tencent Container Security Service (TCSS) เป็นระบบแพตช์เสมือนที่ Tencent Cloud Security พัฒนาขึ้นเพื่อป้องกันช่องโหว่วันศูนย์ (zero-day) ที่เกิดขึ้นบ่อยครั้ง ซึ่งผสานรวมเทคโนโลยีการขุดเจาะช่องโหว่และการแจ้งเตือนช่องโหว่ร้ายแรงแบบเรียลไทม์ของ Tencent ใช้เพื่อตรวจจับและวิเคราะห์ช่องโหว่ สร้างแพตช์เสมือนตามความรู้ความเชี่ยวชาญของ Tencent และทำให้แพตช์เสมือนมีผลบนเซิร์ฟเวอร์คลาวด์โดยอัตโนมัติ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		จรรยาบรรณทางควบคุม ความเสี่ยงที่เพียงพอเหมาะสม	เพื่อป้องกันการโจมตีของแฮกเกอร์ได้อย่างมีประสิทธิภาพ นอกจากนี้ ลูกค้ายังสามารถใช้ Vulnerability Scanning Service (VSS) เพื่อดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของอุปกรณ์เครือข่ายและบริการแอป พลิเคชันขององค์กร และใช้คำแนะนำการแก้ไขที่มีอาชีพลจาก VSS เพื่อลดความเสี่ยงด้านความปลอดภัยขององค์กร เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ดูแล Tencent Cloud ได้สร้างกลไกการสแกนช่องโหว่ภายในและแพลตฟอร์มรวม รวมช่องโหว่ภายนอก Tencent Cloud ใช้ระบบสแกนช่องโหว่เพื่อสแกนช่องโหว่ความปลอดภัยใน สภาพแวดล้อมคลาวด์เป็นประจำ ขอบเขตการสแกนครอบคลุมชั้นเสมือน ชั้นระบบ และชั้นแอปพลิเคชัน ผลการสแกนจะถูกส่งไปยังทีมงานความปลอดภัยของ Tencent Cloud เพื่อใช้ในการวิเคราะห์ จัดประเภท และดำเนินการแก้ไขช่องโหว่ที่พบ สำหรับช่องโหว่ความปลอดภัยที่พบจะถูกบันทึกไว้ในระบบ ใบงาน เพื่อให้มั่นใจว่าช่องโหว่จะได้รับการจัดการและแก้ไขภายใน ระยะเวลาที่กำหนด Tencent Cloud จะระบุแพตช์ล่าสุด และดำเนินการทดสอบความปลอดภัยอย่างเพียงพอก่อน การติดตั้งแพตช์ เพื่อให้มั่นใจในความปลอดภัยของการติดตั้งแพตช์ Tencent Cloud จะแจ้งให้ทีมงานธุรกิจภายในแต่ละทีมทราบเป็นประจำเกี่ยว กับการอัปเดตและติดตั้งแพตช์ และใช้เครื่องมือตรวจจับจุดปลายทาง (endpoint) สแกนสถานะการติดตั้งแพตช์เป็นประจำ และอุปกรณ์ที่ไม่ได้ติดตั้งแพตช์เกินกำหนดเวลาจะถูกสร้า งใบงานแจ้งเตือนโดยอัตโนมัติ
5.1.4	การบริหารจัด การบัญชีผู้ใ งานที่มีสิทธิสู ง	กำหนดมาตรการควบคุมและจ ากัดการใช้บัญชีผู้ใช้งานที่มีสิทธิสูง อย่างเข้มงวด เช่นการมอบหมายสิทธิการเบิกใช้	ลูกค้าควรสร้างกลไกการจัดการผู้ใช้ที่มีสิทธิพิเศษ เพื่อควบคุมการจัดสรรและการให้สิทธิ์ การกำหนดระยะเวลาการใช้งาน และการตรวจสอบการดำเนินการของบัญชีที่มีสิทธิพิเศษ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		กำหนดระยะเวลาการใช้งาน การสอบทานหลังการใช้การกำหนดรหัสผ่าน รหัสกลุ่มของระบบปฏิบัติการ ระบบฐานข้อมูลระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัย เครือข่ายเพื่อป้องกันการนำบัญชีผู้ใช้งานที่มีสิทธิ์สูงไปใช้โดยไม่ได้รับอนุญาต	ป้องกันไม่ให้บัญชีที่มีสิทธิ์สูงถูกใช้โดยไม่ได้รับอนุญาต สำหรับผู้ที่มีสิทธิ์สูง ลูกค้าสามารถใช้ Cloud Access Management (CAM) เพื่อมอบสิทธิ์การเข้าถึงทรัพยากรให้กับผู้ใช้ย่อยผ่านวิธีการต่างๆ เช่น แท็ก เพื่อให้บรรลุการควบคุมการเข้าถึงทรัพยากรคลาวด์อย่างละเอียด CAM ยังสนับสนุนการดูและติดตามบันทึกการดำเนินการของพนักงานผ่าน CloudAudit นอกจากนี้ Tencent Cloud ยังให้บริการ Bastion Host (BH) ที่สามารถสนับสนุนการอนุญาตอย่างละเอียดตามมิติต่างๆ เช่น ผู้ใช้ สิทธิ์ทรัพยากร บัญชีผู้ใช้ และสิทธิ์การดำเนินการ เพื่อให้มั่นใจว่าสิทธิ์ที่ผู้ใช้มีอยู่เป็นสิทธิ์ขั้นต่ำที่จำเป็นสำหรับการเข้าถึงสิทธิ์และทำงานให้สำเร็จ เครื่องบินคุ้มกัน ยังสนับสนุนฟังก์ชันการตรวจสอบการดำเนินการโดยบันทึกและวิเคราะห์บันทึกการดำเนินการของผู้ใช้ เพื่อให้แน่ใจว่าสามารถติดตามเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ภายใน Tencent Cloud ยังได้กำหนดข้อกำหนดการจัดการสำหรับสิทธิ์การเข้าถึงพิเศษและสร้างกลไกการอนุญาตที่เกี่ยวข้อง ในเวลาเดียวกัน Tencent Cloud ได้ปรับใช้เครื่องบินคุ้มกัน อย่างเต็มที่ในสภาพแวดล้อมการผลิต โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบและบีกเอนด์จากส่วนกลางผ่าน เครื่องบินคุ้มกัน การเข้าถึงเครื่องบินคุ้มกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติการอนุญาต เจ้าหน้าที่ปฏิบัติการภายในบางส่วนของ Tencent Cloud เท่านั้นที่สามารถเข้าถึงได้และการเข้าสู่ระบบ เครื่องบินคุ้มกัน ต้องการการยืนยันตัวตนสองปัจจัย กำหนดนโยบายรหัสผ่านสำหรับบัญชีพนักงานตามเส้นฐานความปลอดภัย บันทึกการดำเนินการปฏิบัติการจะถูกเก็บไว้โดยศูนย์กลางแพลตฟอร์มบันทึก (log) และได้รับการตรวจสอบโดยทีมตรวจสอบภายในของ Tencent Cloud เป็นประจำ Tencent Cloud จะรักษานโยบายข้อมูลตัวตนของบุคลากรที่สอดคล้องกับ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			บทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดงานตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์
5.1.5	การพิสูจน์ตัวตนแบบ multi-factor authentication	จัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้ (1) บัญชีผู้ใช้งานที่มีสิทธิ์สูง(privileged user) ทุกบัญชีของระบบปฏิบัติการ ระบบฐานข้อมูลระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย (2) บัญชีผู้ใช้งาน (user) ทุกบัญชีที่สามารถเข้าถึงข้อมูลลูกค้าของระบบ ปฏิบัติการ ระบบฐานข้อมูลระบบงาน อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ที่เชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) หากมีเหตุที่ระบบปฏิบัติการ ระบบฐานข้อมูลระบบงาน อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication ผู้ให้บริการและผู้ประกอบธุรกิจสามารถใช้อิทธิพลอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย อย่างไรก็ตาม กรณีที่ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้นและดำเนินการประเมินความเสี่ยงรวมทั้งพิจารณาแนวทาง ควบคุมความเสี่ยงที่เพียงพอเหมาะสม	ลูกค้าควรใช้การพิสูจน์ตัวตนหลายปัจจัยสำหรับบัญชีผู้ใช้ที่มีสิทธิ์สูงและบัญชีที่เข้าถึงข้อมูลผ่านอินเทอร์เน็ต ในด้านการจัดการบัญชีผู้ใช้และการให้สิทธิ์ Cloud Access Management (CAM) สามารถช่วยลูกค้าจัดการการเข้าถึงผลิตภัณฑ์และบริการของ Tencent Cloud ได้อย่างปลอดภัยและละเอียดรอบคอบ รองรับฟังก์ชันการตรวจสอบยืนยันตัวตนขั้นที่สองหลายวิธี รวมถึงการใช้การตรวจสอบโดยอุปกรณ์ MFA หรือการตรวจสอบด้วยรหัสยืนยันทางโทรศัพท์ เพื่อยืนยันความปลอดภัยของตัวตนและสภาพแวดล้อมก่อนเข้าสู่ระบบและดำเนินการที่ละเอียดอ่อน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ยังได้กำหนดกลยุทธ์การให้สิทธิ์การควบคุมการเข้าถึงและกลไกเมทริกซ์การแบ่งแยกสิทธิ์ภายในองค์กร ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการยืนยันตัวตนสองปัจจัยสำหรับบัญชีผู้ใช้ที่เข้าสู่ระบบ สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้ เครื่องบินคุ้มกัน อย่างเต็มรูปแบบ โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบแบบปิดเอนต์จากส่วนกลางผ่าน เครื่องบินคุ้มกัน การเข้าถึงเครื่องบินคุ้มกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติสิทธิ์ มีเฉพาะเจ้าหน้าที่ปฏิบัติการภายในของ Tencent Cloud บางส่วนเท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบ เครื่องบินคุ้มกัน ต้องการการยืนยันตัวตนสองปัจจัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
5.1.6	การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ	จัดให้มีการประเมินช่องโหว่ (vulnerability assessment) สำหรับทุกระบบงานตามระดับความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งทดสอบ เจาะระบบ (penetration test) โดยผู้เชี่ยวชาญที่มีความเป็นอิสระครอบคลุมระบบงานและระบบเครือข่าย ที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) อย่างน้อยปีละ 1 ครั้ง และทุกครั้ง ที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความเสี่ยง หรือมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ อย่างมีนัยสำคัญ ทั้งนี้ เพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไข และป้องกันภัยคุกคามที่อาจเกิดขึ้นได้อย่างทันการณ์ ทั้งนี้ ในกรณีที่ กระทบ. เห็นว่าผลการทดสอบเจาะระบบมีข้อมูลรายงานไม่ครบถ้วน ขอบเขตหรือวิธีการทดสอบการเจาะระบบไม่ครอบคลุมช่องโหว่ที่สำคัญที่เป็นความเสี่ยงที่ได้รับการยอมรับ โดยทั่วไป หรือในกรณีที่ กระทบ. เห็นว่า เป็นหรือสมควร กระทบ. อาจสั่งให้แต่งตั้งผู้เชี่ยวชาญภายนอกที่มีความเป็นอิสระดำเนินการทดสอบเจาะระบบเพิ่มเติมได้	ลูกค้าควรดำเนินการประเมินช่องโหว่และการทดสอบเจาะระบบเป็นประจำ เพื่อระบุช่องโหว่ด้านความปลอดภัยและประเมินความสามารถในการป้องกันความปลอดภัยทางไซเบอร์ของตน ในด้านการทดสอบเจาะระบบ Tencent Cloud ให้บริการ Penetration Testing Service (PTS) แก่ลูกค้า ด้วยการจำลองเทคนิคการโจมตีและเทคนิคการค้นพบช่องโหว่ที่แฮกเกอร์อาจใช้อย่างเต็มรูปแบบ ใช้วิธีการและกลไกที่ควบคุมได้และไม่ทำลายล้างเพื่อทำการตรวจสอบความปลอดภัยของระบบเป้าหมายอย่างลึกซึ้ง ค้นหาจุดอ่อนที่มีอยู่ในเป้าหมายและอุปกรณ์เครือข่าย ให้คำแนะนำในการเสริมความแข็งแกร่งด้านความปลอดภัยเพื่อช่วยลูกค้ายกระดับความปลอดภัยของระบบ และสนับสนุนการตรวจสอบหลังการแก้ไขช่องโหว่ ในด้านการสแกนช่องโหว่ ลูกค้าสามารถเลือกใช้ Vulnerability Scanning Service (VSS) เพื่อตรวจสอบสินทรัพย์เครือข่ายขององค์กรและระบุความเสี่ยงของสินทรัพย์นั้นๆ โดยใช้ประโยชน์จากประสบการณ์ด้านความปลอดภัยและข่าวกรองภัยคุกคามที่สะสมมาหลายปีของ Tencent Cloud VSS ได้สร้างฐานข้อมูลกฎช่องโหว่ที่อุดมสมบูรณ์และครอบคลุม และมีความสามารถในการตรวจจับช่องโหว่ 0Day/1Day/NDay ที่มีอาชีพและมีประสิทธิภาพสูง สามารถดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของสินทรัพย์ของลูกค้า ให้คำแนะนำการแก้ไขที่มีอาชีพแก่ลูกค้า เพื่อลดความเสี่ยงด้านความปลอดภัย VSS ยังสนับสนุนการทำงานร่วมกับผลิตภัณฑ์คลาวด์ เช่น ความปลอดภัยโฮสต์ ไฟร์วอลล์แอปพลิเคชันเว็บ เพื่อให้บรรลุวงจรปิดจากการตรวจสอบความเสี่ยงไปจนถึงการจัดการความเสี่ยง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะสร้างงานสแกนเป็นประจำผ่านระบบสแกนช่องโหว่เพื่อสแกนช่องโหว่ของสินทรัพย์ในสภาพแวดล้อมคลาวด์ และวิเคราะห์ จัดประเภท

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และดำเนินการแก้ไขช่องโหว่ที่พบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะดำเนินการทดสอบเจาะระบบขนาดใหญ่แบบเต็มวงจรเป็นประจำ และดำเนินการทดสอบเจาะระบบแบบเจาะจงอย่างยืดหยุ่นในสถานการณ์ต่างๆ เช่น ก่อนการเปิดตัวผลิตภัณฑ์ใหม่หรือเมื่อมีการเปลี่ยนแปลงครั้งสำคัญ ผลการทดสอบเจาะระบบจะแจ้งให้ฝ่ายงานผู้รับผิดชอบที่เกี่ยวข้องทราบในวงความปลอดภัย และฝ่ายงานผู้รับผิดชอบจะดำเนินการปะช่องโหว่หรือดำเนินการมาตรการควบคุมขุดเซย์อื่นๆ ทันที เพื่อให้มั่นใจว่าช่องโหว่ที่ใช้ประโยชน์ได้ซึ่งพบในการทดสอบเจาะระบบได้รับการจัดการอย่างเหมาะสม นอกจากนี้ Tencent Cloud ยังดำเนินการฝึกซ้อมการต่อสู้เสมือนระหว่างทีมแดงและทีมน้ำเงินเพื่อจำลองการต้านทานการโจมตีทางเครือข่ายเป็นประจำ Tencent Cloud ยังได้สร้างแพลตฟอร์มรับข้อเสนอแนะช่องโหว่จากภายนอกและดำเนินการ "โครงการให้รางวัลการรายงานช่องโหว่" โดยเชิญผู้เชี่ยวชาญด้านความปลอดภัยในอุตสาหกรรมช่วย Tencent Cloud ค้นพบช่องโหว่และความเสี่ยงด้านความปลอดภัยของระบบจากมุมมองของแฮกเกอร์ เพื่อแก้ไขปัญหาด้านความปลอดภัยได้ทันทั่วทั้งและบำรุงรักษาความปลอดภัยของระบบนิเวศของ Tencent Cloud

8.2 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
5.2.1	ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ	จัดให้มีโครงสร้างและบทบาทหน้าที่ความรับผิดชอบในการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม	ลูกค้าควรสร้างโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ชี้แจงบทบาทและความรับผิดชอบของคณะกรรมการและผู้บริหารระดับสูง และกำหนดนโยบายการกำกับดูแลความเสี่ยงด้านเทคโนโลยี

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ตั้งแต่คณะกรรมการและผู้บริหารระดับสูงที่ให้ความสำคัญกับความปลอดภัยในการผลักดันและยกระดับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กำหนดให้มีความเกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ลยสารสนเทศ โดยฝ่ายบริหารควรกำกับดูแลการดำเนินการตามนโยบายดังกล่าว นอกจากนี้ ลูกค้ายังควรแต่งตั้งบุคคลเฉพาะรับผิดชอบด้านการจัดการความปลอดภัยเทคโนโลยีสารสนเทศ และสร้างวัฒนธรรมการตระหนักรู้เกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศภายในองค์กร
		สื่อสารและกำกับดูแลให้มีการปฏิบัติตามนโยบายที่กำหนด นอกจากนี้ต้องจัดให้มีผู้รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งสร้างวัฒนธรรมและพฤติกรรมรวมของทุกคนในองค์กรให้ตระหนักถึงความเสี่ยงอย่างต่อเนื่อง	เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดการกำกับดูแล ในด้านกลยุทธ์ความปลอดภัยทางไซเบอร์ เพื่อรับมือกับภัยคุกคามทางเครือข่ายและความเสี่ยงด้านความปลอดภัยที่ซับซ้อนมากขึ้นในยุคดิจิทัล Tencent Cloud ได้เปิดตัวกรอบแบบจำลอง "ภูมิคุ้มกันปลอดภัยดิจิทัล" เสนอให้ใช้แนวคิดด้านภูมิคุ้มกันในการรับมือกับความซับซ้อนเชิงประสานงานระหว่างการสร้างความปลอดภัยและการพัฒนาธุรกิจยุคใหม่ โดยกำหนดเป้าหมายที่ข้อมูลและธุรกิจขององค์กร เพื่อสร้างระบบภูมิคุ้มกันความปลอดภัยที่มีความยืดหยุ่นปรับตัวได้ และขยายได้ ช่วยคุ้มครองการพัฒนาคุณภาพสูงขององค์กรในยุคดิจิทัล
			Tencent Cloud มีเป้าหมาย "เสริมสร้างภูมิคุ้มกันปลอดภัยดิจิทัลขององค์กร" สนับสนุนการพัฒนาที่มีความยืดหยุ่นในยุคดิจิทัล" มุ่งมั่นปรับปรุงระบบความปลอดภัยบนคลาวด์ของตนเอง สร้างขีดความสามารถด้านความปลอดภัยและการปฏิบัติตามข้อกำหนด และกำหนดมาตรฐานความปลอดภัยบนคลาวด์ โดยอิงตามกรอบแบบจำลองที่วางแผนอย่างครอบคลุมผ่านผลิตภัณฑ์ที่หลากหลายและคุณลักษณะด้านความปลอดภัย Tencent Cloud บริหารการป้องกันในทุกด้าน และนำฟังก์ชันความปลอดภัยที่สอดคล้องกันไปใช้ในผลิตภัณฑ์ทุกระดับ
			Tencent Cloud ได้จัดตั้งคณะกรรมการเทคโนโลยีความปลอดภัยและทีมงานความปลอดภัยมืออาชีพที่มีหน้าที่และสาขาวิชาที่แตกต่างกัน และได้สร้างมาตรฐานและขั้นตอนการจัดการทรัพยากรบุคคลที่สมบูรณ์ภายในองค์กร เพื่อให้มั่นใจในการคัดเลือกจ้าง และจัดวางบุคลากรตามข้อกำหนดของตำแหน่งงาน Tencent Cloud

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
5.2.2	การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ		รวบรวมทีมบริการผู้เชี่ยวชาญที่มีประสบการณ์ในอุตสาหกรรม มุ่งมั่นให้บริการผลิตภัณฑ์และบริการที่ปลอดภัย น่าเชื่อถือ เป็นมืออาชีพ และเป็นไปตามข้อกำหนดแก่ลูกค้า นอกจากนี้ Tencent Cloud ยังได้จัดเตรียมเส้นทางพัฒนาอาชีพที่หลากหลาย จัดเตรียมทรัพยากรการเรียนรู้ที่อุดมสมบูรณ์และมีคุณภาพสูงให้กับพนักงาน ปรับปรุงหลักสูตรและระบบการฝึกอบรมอย่างต่อเนื่อง เพื่อสนับสนุนการเติบโตส่วนบุคคลและพัฒนาอาชีพของพนักงาน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำกับดูแลเทคโนโลยีสารสนเทศ โปรดดูบทที่ 5.2 "5.2 เอกสารแนบ 1 ธรรมชาติของเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
		จัดให้มีการบริหารจัดการและควบคุมระบบเทคโนโลยีสารสนเทศที่รองรับการให้บริการให้มีความปลอดภัย ถูกต้องเชื่อถือได้ และพร้อมใช้งาน โดยนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการและผู้ประกอบธุรกิจ	ลูกค้าควรกำหนดและบำรุงรักษานโยบาย มาตรฐาน และขั้นตอนด้านความปลอดภัยทางเทคโนโลยี เพื่อบริหารจัดการและควบคุมระบบเทคโนโลยีสารสนเทศ ที่สนับสนุนการดำเนินงานของบริการ และควรทบทวนและปรับปรุงนโยบายและกระบวนการเหล่านี้เป็นประจำ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดการกำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูล ซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยข้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดการความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ รวมถึงชั้นนำการทำงานประจำวันและกระบวนการจัดการของหน่วยงานและพนักงานทุกหน่วยในบริษัท นโยบายความปลอดภัยข้อมูลของ Tencent Cloud จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัยบนคลาวด์สอดคล้องกับนโยบายความปลอดภัย มาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบายความปลอดภัยข้อมูล สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการความปลอดภัย

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
5.2.3	การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ		เทคโนโลยีสารสนเทศ โปรดดูบทที่ 5.3 "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
		จัดให้มีการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างครอบคลุมทั่วทั้งองค์กรและเหมาะสมกับระดับความเสี่ยงที่ยอมรับได้ โดยกำหนดนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมโครงสร้างองค์กร บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและต้องปฏิบัติตามนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ลูกค้าควรกำหนดระบบการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดำเนินการปฏิบัติการจัดการความเสี่ยงและมาตรการควบคุมที่มีประสิทธิภาพ ชี้แจงผู้รับผิดชอบที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และทบทวนนโยบายการจัดการความเสี่ยงเป็นประจำ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามงานต่างๆ เช่น การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยงไว้อย่างชัดเจน Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุความเสี่ยงตามสถานการณ์ความเสี่ยง ผลกระทบทางธุรกิจ หรือกระบวนการให้บริการ สำหรับความเสี่ยงที่ระบุได้ Tencent Cloud จะประเมินความเป็นไปได้และระดับผลกระทบของความเสี่ยงแต่ละรายการเพื่อจำแนกระดับความเสี่ยง และดำเนินการตามขั้นตอนที่สอดคล้องกันต่อไป โดยมีการบันทึกกิจกรรมกระบวนการทั้งหมดไว้ Tencent Cloud ยังติดตามสถานการณ์การจัดการความเสี่ยงอย่างต่อเนื่อง ประเมินความเสี่ยงที่เหลืออยู่ และให้มั่นใจว่าผู้เกี่ยวข้องได้จัดการความเสี่ยงอย่างเหมาะสมตามข้อกำหนดการจัดการความเสี่ยงของ Tencent Cloud นอกจากนี้ Tencent Cloud บำรุงรักษาและปรับปรุงวิธีการประเมินความเสี่ยงและทะเบียนความเสี่ยงอย่างต่อเนื่องตามแนวโน้มการเปลี่ยนแปลงในอุตสาหกรรมตลาดและแนวปฏิบัติการจัดการภายใน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โปรดดูบทที่ 5.4 "5.4 เอกสารแนบ 3

ลำดับที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
5.2.4	การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ	กำกับดูแลให้ปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ (IT compliance)	การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ ในคู่มือนี้ ลูกค้าควรกำกับดูแลการปฏิบัติตามกฎหมายระเบียบข้อบังคับและข้อกำหนดทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศของตน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด และได้สร้างขั้นตอนที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านความปลอดภัย เพื่อให้มั่นใจว่าการดำเนินการด้านความปลอดภัยข้อมูลเป็นไปตามข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ มาตรฐาน และขั้นตอนที่เกี่ยวข้อง ทีมงานฝ่ายกฎหมายของ Tencent Cloud จะระบุและรวบรวมข้อกำหนดการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับธุรกิจของ Tencent Cloud อย่างต่อเนื่อง จัดทำเป็นรายการกฎหมายและระเบียบข้อบังคับที่สอดคล้องกัน และบำรุงรักษาและปรับปรุงเป็นประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศ โปรดดูบทที่ 5.5 "5.5 เอกสารแนบ 4 การกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
		เช่นกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์หรือกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง	ลูกค้าควรสร้างกลไกการตรวจสอบเทคโนโลยีสารสนเทศดำเนินการตรวจสอบความเสี่ยงทางเทคนิคเป็นประจำและติดตามการดำเนินการแก้ไขปัญหาที่พบในการตรวจสอบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบการจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และ
5.2.5	การตรวจสอบด้านเทคโนโลยีสารสนเทศ	จัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยผู้ตรวจสอบที่มีความเป็นอิสระ รวมทั้งต้องติดตามให้มีการปรับปรุงประเด็นจากการตรวจสอบเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัย การบริหารความเสี่ยงและการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ที่เพียงพอ	ลูกค้าควรสร้างกลไกการตรวจสอบเทคโนโลยีสารสนเทศดำเนินการตรวจสอบความเสี่ยงทางเทคนิคเป็นประจำและติดตามการดำเนินการแก้ไขปัญหาที่พบในการตรวจสอบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบการจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และ

ลำดับ ที่	โดเมนกา รควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อ กำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็น อิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มี ลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการ ล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่ สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดเอกสารงานล่าสุดได้ด้วยตนเองจา ก " Compliance Document Download" สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบเทคโนโลยีสาร สนเทศ โปรดดูบทที่ 5.6 "5.6 เอกสารแนบ 5 การตรวจสอบด้านเทคโนโลยีสารสนเทศของสถาบันการ เงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้

8.3 การแจ้งหรือรายงานต่อปท.

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
7.1	การแจ้งการนาเทคโนโลยีมาใช้หรือเปลี่ยนแปลงระบบหรือเทคโนโลยีสารสนเทศที่สำคัญ	ผู้ให้บริการต้องแจ้งการนาเทคโนโลยีมาใช้หรือเปลี่ยนแปลงระบบหรือเทคโนโลยี สารสนเทศที่มีนัยสำคัญทั้งหมดที่ดำเนินการเองและกรณีที่มีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ต่อปท. ล่วงหน้า 15 วันก่อนดำเนินการตามช่องทางที่อปท. กำหนด	ลูกค้าที่จะนาเทคโนโลยีที่สำคัญมาใช้หรือจะมีการเปลี่ยนแปลงครั้งใหญ่ในระบบเทคโนโลยีสารสนเทศ ไม่ว่าการเปลี่ยนแปลงนั้นจะดำเนินการโดยตนเองหรือโดยผู้ให้บริการบุคคลที่สาม ต้องแจ้งผ่านทางที่ธนาคารแห่งประเทศไทยกำหนดอย่างน้อย 15 วันก่อนการดำเนินการ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอการดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และขอบเขตของการเปลี่ยนแปลง สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแวดล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขยาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม
7.2	การรายงานปัญหาด้านเทคโนโลยีสารสนเทศ	ผู้ให้บริการต้องรายงานต่ออปท. ในกรณีที่เกิดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญ ในการใช้เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบต่อการใช้งาน หรือชื่อเสียงรวมถึงกรณีเทคโนโลยีสารสนเทศที่มีนัยสำคัญถูกโจมตีหรือถูกขโมยจากภัยคุกคามทางไซเบอร์และเป็นปัญหาหรือเหตุการณ์ที่ต้องรายงานต่อผู้บริหารในตำแหน่งสูงสุดโดยผู้ให้บริการต้องรายงานปัญหาหรือเหตุการณ์ดังกล่าวมายังอปท. ทันทีเมื่อเกิดเหตุหรือรับรู้ปัญหาหรือเหตุการณ์นั้นตามช่องทางที่อปท. กำหนด และแจ้งสาเหตุและการแก้ไขปัญหาเพิ่มเติมภายหลัง	ลูกค้าที่เกิดหรือพบปัญหาหรือเหตุการณ์สำคัญด้านเทคโนโลยีสารสนเทศต้องแจ้งผ่านช่องทางที่ธนาคารแห่งประเทศไทยกำหนดทันที และภายหลังต้องชี้แจงเพิ่มเติมถึงสาเหตุของเหตุการณ์และมาตรการแก้ไข เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการสื่อสารและการแจ้งเหตุการณ์ Tencent Cloud ได้กำหนดมาตรฐานการจัดการเหตุการณ์ความปลอดภัยข้อมูล สร้างขั้นตอนที่เกี่ยวข้อง เช่น การตอบสนองเหตุการณ์ความปลอดภัยข้อมูล การยกระดับเหตุการณ์ และการแจ้งเหตุการณ์ เพื่อแจ้งเตือนหรือแจ้งให้พนักงานภายในบริษัท ลูกค้า และผู้เกี่ยวข้องอื่น ๆ ที่อาจหรือได้รับผลกระทบจากอุบัติเหตุทราบทันเวลา ทำให้ทุกฝ่ายสามารถสื่อสารและประสานงานกันอย่างเป็นระเบียบ ทันเวลา และมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้เหลือน้อยที่สุด ในด้านการที่ลูกค้าแจ้งปัญหาหรือติดต่อ Tencent Cloud คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการโบบาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ระบบใบงานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับใบงานของลูกค้าผ่านกลไกการตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมและจัดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้าได้รับการตอบสนองและจัดการอย่างทันทั่วถึง นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้าได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเวลา ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับการสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า
7.3	การรายงานผลการประเมิน การปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ	ผู้ให้บริการระบบการชำระเงินที่มีความสำคัญผู้ประกอบการชำระเงินภายใต้ การกำกับและผู้ประกอบการบริการการชำระเงินภายใต้การกำกับที่มีนัยสำคัญต้องจัดส่งผลการประเมิน การปฏิบัติตามหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศทั้งในส่วนหลักเกณฑ์ การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น(Cyber Hygiene) และ หลักเกณฑ์การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ผู้ให้บริการบริการชำระเงินที่อยู่ภายใต้การกำกับดูแลซึ่งไม่ใช่ระบบการชำระเงินที่สำคัญ	ลูกค้าควรจัดทำและส่งรายงานตามรูปแบบและระยะเวลาที่ธนาคารแห่งประเทศไทยกำหนด และภายใน 30 วันนับจากสิ้นปีปฏิทินทุกปี ต้องส่งรายงานประเมินการปฏิบัติตามข้อกำหนดการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศตามรูปแบบและช่องทางที่ธนาคารแห่งประเทศไทยกำหนด Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเทศไทย ปัจจุบัน Tencent Cloud ได้รับการรับรองและคุณวุฒิด้านความปลอดภัยและความเป็นส่วนตัวหลายรายการผ่านการตรวจสอบหรือประเมินโดยบุคคลที่สามที่เป็นอิสระ และตามความต้องการของลูกค้า

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ต้องจัดส่งผลการประเมิน เฉพาะหลักเกณฑ์การรักษาความม ั่นคงปลอดภัยของระบบเทคโนโลยีสา รสนเทศขั้นต้นที่จ ำเป็น(Cyber Hygiene) โดยจัดส่งผลการประเมินให้อปท. ทราบภายใน 30 วันนับแต่วั นสิ้นปีปฏิทินโดยมีรูปแบบและ ช่องทางตามที่อปท. กำหนด	โดยผ่านการจัดทำรายงานการควบคุมระบบและองค์กรที่ มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริกร ล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่ สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจาก ก " Compliance Document Download "
7.4	การรายงานบุ คคลภายนอก ที่มีนัยสำคัญ	ผู้ให้บริการระบบการชำระเงินที่มีคว ามส าคัญ ผู้ประกอบการธุรกิจระบบการชำระเงินภ ายใต้ การกำกับ และผู้ประกอบธุรกิจบริการการชำระ เงินภายใต้การกำกับที่มีนัยส าคัญต้องจัดส่งรายงาน การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลของบุคคลภาย นอกที่มีนัยส าคัญเป็นรายไตรมาส ตามรูปแบบและช่องทางที่ อปท. ก าหนด	ลูกค้าที่ได้รับการจัดประเภทเป็นผู้ให้บริการระบบการชำระ เงินที่สำคัญ ผู้ให้บริการระบบการชำระเงินที่อยู่ภายใต้การกำกับดูแล และผู้ให้บริการบริการชำระเงินที่สำคัญซึ่งอยู่ภายใต้การ กำกับดูแล ต้องรายงานสถานการณ์การใช้บริการของบุคคลที่สามที่ สำคัญเป็นประจำทุกไตรมาสตามรูปแบบและช่องทางที่ธ าการแห่งประเทศไทยกำหนด Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์ จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเท ศไทย

09

Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับหลักเกณฑ์ทั่วไปในการกำกับดูแล

การประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับของ BOT อย่างไร

ธนาคารแห่งประเทศไทยได้จัดทำ [BOT No. SorNorChor 6/2561](#) เรื่อง [หลักเกณฑ์ทั่วไปในการกำกับดูแล การประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ](#) ซึ่งกำหนดกรอบการกำกับดูแลสำหรับการดำเนินงานของธุรกิจ บริการชำระเงินที่กำหนด⁵ โดยชัดเจน เพื่อให้ผู้ให้บริการธุรกิจมุ่งเน้นไปที่สี่ด้าน ได้แก่ สภาพทางการเงิน การกำกับดูแลภายใน การจัดการความเสี่ยงและความปลอดภัย และการปกป้องสิทธิประโยชน์ของผู้ใช้ เพื่อเพิ่มขีดความสามารถในการแข่งขันและประสิทธิภาพของผู้ให้บริการธุรกิจ

ในบทนี้ Tencent Cloud จะสรุปและรวบรวมข้อกำหนดความคุ้มครองที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จากหลักเกณฑ์ทั่วไปในการกำกับดูแล การประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับ และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud จะช่วยสถาบันการเงินในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดความคุ้มครองเฉพาะ	การตอบสนองของ Tencent Cloud
4.2.3 (1)	นโยบายการจัด การความเสี่ยง	(1) กำหนดนโยบายการบริหารความ เสี่ยงในการให้บริการการชำระ เงิน อย่างชัดเจนและเป็นลายลักษณ์อ ักษร ให้สอดคล้องกับรูปแบบธุรกิจ ขนาด ปริมาณธุรกรรม และ ความซับซ้อนของการให้บริการ โดยต้องได้รับความเห็นชอบจากค ณะกรรมการบริษัทหรือ คณะกรรมการที่ได้รับมอบหมาย รวมทั้งต้องมีการกำหนดแนวทาง วิธีการ ผู้รับผิดชอบในการบริหาร ความเสี่ยง ประเมินผลการปฏิบัติตามแนวท างและวิธีการที่กำหนด และต้องรายงานผลการปฏิบัติ ดังกล่าวให้คณะกรรมการบริษัท หรือคณะกรรมการ หรือผู้บริหารที่ได้รับมอบหมายท ราบภายใน ระยะเวลาที่เหมาะสม	ลูกค้าควรกำหนดนโยบายการจัดการความเสี่ยงสำหรับ บริการชำระเงินที่สอดคล้องกับรูปแบบธุรกิจ ขนาด ปริมาณธุรกรรม และระดับความซับซ้อนของธุรกิจ และได้รับการอนุมัติจากคณะกรรมการหรือคณะกรรมการกา รที่กำหนด และรายงานผลการจัดการความเสี่ยงเป็นประจำต่อคณะก รรมการ คณะกรรมการ หรือฝ่ายบริหารที่ได้รับมอบอำนาจ Tencent Cloud พัฒนาและบำรุงรักษากรอบการจัดการความเสี่ยงภายใน ตามมาตรฐาน ISO/IEC 27001:2022 เพื่อระบุ วิเคราะห์ และจัดการความเสี่ยงที่ระบุไว้ Tencent Cloud ดำเนินการประเมินความเสี่ยงอย่างเป็นทางการอย่างน้อย ปีละหนึ่งครั้ง สำหรับความเสี่ยงที่ระบุได้ จะให้คะแนนตามมูลค่าสินทรัพย์ ความเป็นไปได้ที่ความเสี่ยงจะเกิดขึ้น และระดับผลกระทบของความเสี่ยง เพื่อคำนวณระดับความเสี่ยง จากผลการวิเคราะห์ความเสี่ยง จะจัดเตรียมกลยุทธ์การตอบสนองและมาตรการบรรเทา ความเสียหายที่สอดคล้องกันสำหรับความเสี่ยงที่ระบุ เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

⁵ บริการชำระเงินที่กำหนด: การบริการชำระเงินที่กำหนด ตามมาตรา 16 แห่งพระราชบัญญัติระบบการชำระเงิน ประกอบด้วยธุรกิจ 6 ประเภทหลัก ได้แก่ บริการบัตรเครดิต บัตรเดบิต หรือบัตร ATM บริการเงินอิเล็กทรอนิกส์ การรับชำระเงินอิเล็กทรอนิกส์แทนผู้ขาย/ผู้ให้บริการ/เจ้าหนี้ – ซึ่งหมายถึงการรับชำระเงิน (Acquiring) หรือบริการอำนวยความสะดวกในการชำระเงิน การโอนเงินผ่านช่องทางอิเล็กทรอนิกส์ – ซึ่งหมายถึงการโอนเงินทางอิเล็กทรอนิกส์ บริการชำระเงินอื่นๆ ที่อาจส่งผลกระทบต่อระบบการเงินหรือประโยชน์สาธารณะ

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
4.2.3 (2)	การจัดการความ ต่อเนื่องของธุ รกิจ	(2) จัดให้มีแนวทางการบริหารความ ต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และแผนรองรับการดำเนินธุรกิจอ ย่างต่อเนื่อง (Business Continuity Plan : BCP) เพื่อรองรับกรณีการเกิดปัญหาหรือ เหตุการณ์ผิดปกติ ให้สอดคล้องเหมาะสมกับประเภท และความซับซ้อนของการประกอบธุ รกิจเพื่อลดผลกระทบที่อาจเกิดขึ้น	ลูกค้าควรสร้างกลยุทธ์การจัดการความต่อเนื่องของธุรกิจ และแผนความต่อเนื่องของธุรกิจที่สอดคล้องกับประเภท และระดับความซับซ้อนของธุรกิจ เพื่อรับมือกับปัญหาหรือเหตุการณ์ต่างๆ ที่อาจเกิดขึ้น เพื่อให้มั่นใจว่าลูกค้าสามารถตอบสนองและกู้คืนฟังก์ชัน สำคัญได้อย่างรวดเร็วหลังเกิดเหตุการณ์ภัยพิบัติ ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud ให้มา เช่น บริการคอมพิวเตอร์ บริการเครือข่าย บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ บริการความปลอดภัย ล้วนมีคุณลักษณะความพร้อมใช้งานสูง และมีแผนการกู้คืนจากภัยพิบัติที่สอดคล้องกัน เช่น: • Cloud Load Balancer (CLB) ให้บริการกระจายปริมาณข้อมูลระดับ 4 และ 7 ที่ปลอดภัยและรวดเร็ว โดยขยายความสามารถในการให้บริการภายนอกข องระบบแอปพลิเคชันผ่านการกระจายปริมาณข้อมูล และจัดจุดเชื่อมต่อเพียงจุดเดียว CLB ใช้การปรับใช้แบบคลัสเตอร์ และจะลบอินสแตนซ์ที่ขัดข้องออกทันทีทางที่ เพื่อให้บรรลุความพร้อมใช้งานสูง • Cloud Virtual Machine (CVM) มีคุณลักษณะของความพร้อมใช้งานสูงของบริการแ ละความน่าเชื่อถือสูงของข้อมูล Cloud Block Storage ที่ใช้กับ CVM ให้กลยุทธ์การจัดเก็บข้อมูลสำรองสามชุด ซึ่งรับประกันความสามารถในการย้ายและกู้คืนข้อมูล ได้อย่างรวดเร็วเมื่อสำเนาใดสำเนาหนึ่งขัดข้อง • Cloud Object Storage (COS) ให้การจัดเก็บข้อมูลสำรองหลายชุดผ่านหลายสถา ปัตยกรรมและหลายอุปกรณ์ จัดเตรียมฟังก์ชันการกู้คืนจากภัยพิบัติข้ามพื้นที่แล ะการแยกทรัพยากรสำหรับข้อมูลลูกค้า และให้บรรลุความคงทนของข้อมูล • TencentDB for MySQL รองรับความน่าเชื่อถือสูงของข้อมูลและความพร้อมใ ใช้งานสูงของบริการ และมีกลไกการสำรองข้อมูลอัตโนมัติและการกู้คืนโด ยไม่สูญเสียข้อมูลที่สมบูรณ์

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			<u>Tencent Kubernetes Engine (TKE)</u> ใช้สถาปัตยกรรมบริการแบบกระจาย รับประกันการกู้คืนโดยอัตโนมัติจากการขัดข้องของ บริการและการย้ายถิ่นฐานอย่างรวดเร็ว ผสานกับที่เก็บข้อมูลแบบกระจายสำหรับบริการแบบ มีสถานะ (Stateful) เพื่อให้บรรลุความปลอดภัยและความพร้อมใช้งานสูง ของบริการและข้อมูล เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ดูแล Tencent Cloud มีการแยกจากกันโดยสมบูรณ์ระหว่างภูมิภาคต่างๆ เพื่อรับประกันความเสถียรและความทนทานต่อข้อผิดพลาด สูงสุดระหว่างภูมิภาคต่างๆ เพื่อให้มั่นใจในความพร้อมใช้งานสูงของข้อมูล Tencent Cloud แบ่งแต่ละภูมิภาคออกเป็นหลาย Availability Zone ที่แยกจากกัน การออกแบบหลาย Availability Zone ของ Tencent Cloud สามารถลดผลกระทบจากความล้มเหลวของจุดเดียวได้ อย่างมีประสิทธิภาพ และรับประกันว่าความล้มเหลวระหว่าง Availability Zone จะถูกแยกจากกัน ซึ่งจะช่วยรับประกันความต่อเนื่องของธุรกิจของลูกค้า เพื่อให้มั่นใจในความพร้อมใช้งานอย่างต่อเนื่องของ ธุรกิจลูกค้า Tencent Cloud ได้ออกแบบและนำกรอบการจัดการความต่อเนื่องของธุรกิจ ที่เหมาะสมกับสภาพแวดล้อมคอมพิวเตอร์คลาวด์ของ ตนเองไปใช้ และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจ Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภัณฑ์ และบริการคลาวด์ กำหนด RTO และ RPO ของแต่ละธุรกิจให้ชัดเจน และจัดทำกลยุทธ์การตอบสนองและแผนความต่อเนื่องของ ธุรกิจที่แตกต่างกันตามผลการวิเคราะห์ผลกระทบทางธุรกิจ รวมถึงจัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดย ละเอียดสำหรับผลิตภัณฑ์คลาวด์ Tencent Cloud จะทำการทดสอบฝึกซ้อมความต่อเนื่องของธุรกิจสำหรับ ผลิตภัณฑ์คลาวด์เป็นประจำตามแผนความต่อเนื่องของธุรกิจ เพื่อให้แน่ใจในความสามารถในการปฏิบัติตามได้จริงของแผน แผนฉุกเฉิน ฯลฯ

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
4.2.3 (3)	การตรวจสอบบัน ทึก (Log Audit)	(3) จัดให้มีระบบงานที่สามารถตรวจ สอบรายการย้อนหลังได้	ลูกค้าควรสร้างระบบบันทึกและตรวจสอบ (Logging and Audit) เพื่อให้มั่นใจในความสามารถในการติดตามประวัติ (Traceability) ของบันทึกย้อนหลัง เพื่อช่วยลูกค้าในการรวบรวม สรุป และวิเคราะห์หลักฐานที่เกี่ยวข้องกับเหตุการณ์ Tencent Cloud ให้บริการ Cloud Log Service (CLS) เพื่อช่วยเหลือผู้ใช้ในการแก้ไขปัญหาด้านการดำเนินธุรกิจ การตรวจสอบความปลอดภัย การตรวจสอบบันทึก และการวิเคราะห์บันทึกผ่านบันทึก Tencent Cloud CLS ใช้การออกแบบสถาปัตยกรรมแบบกระจายที่มีความพร้อมใช้งานสูง จัดเก็บข้อมูลบันทึกด้วยการสำรองข้อมูลหลายชุด ป้องกันไม่ให้ข้อมูลไม่สามารถใช้งานได้เมื่อบริการไหนเดี ยวขัดข้อง ให้บริการที่มีความพร้อมใช้งานสูง และรับประกันบริการที่เสถียรและน่าเชื่อถือสำหรับข้อมูล บันทึก นอกจากนี้ บริการ Elasticsearch Service (ES) ผ่านการปรับใช้ในเครือข่ายส่วนตัว Virtual Private Cloud (VPC) ที่แยกออกจากกันทางตรรกะ ลูกค้าสามารถควบคุมการกำหนดค่าสภาพแวดล้อมของ ตนเองได้โดยสมบูรณ์ กำหนด Access Control List (ACL) ของเครือข่ายและ Security Group ตามต้องการ และจัดเตรียมแผนการปรับใช้หลาย Availability Zone ซึ่งสามารถรับประกันว่าเซิร์ฟเวอร์จะไม่หยุดชะงักแม้ในกรณ ที่เครือข่ายหรือไฟฟ้าใน Availability Zone เดียวขัดข้องเนื่องจากเหตุสุดวิสัย สำหรับการรวบรวมและการเก็บรักษบบันทึกเครือข่าย Cloud Firewall (CFW) รองรับการวิเคราะห์บันทึกเครือข่ายของปริมาณข้อมูลทั้งหมด และสามารถเก็บรักษาได้สูงสุด 6 เดือน และรองรับการวิเคราะห์การติดตามภัยคุกคามขั้นสูง ซึ่งสามารถวิเคราะห์ข้อมูลการจดทะเบียนโดเมน การแก้ไข การขึ้นทะเบียน และประวัติการแก้ไขได้ สำหรับการรวบรวมและการเก็บรักษบบันทึกการดำเนินการ ลูกค้าสามารถใช้ CloudAudit เพื่อกำกับดูแลกิจกรรมบัญชี Tencent Cloud ตรวจสอบความสอดคล้อง ตรวจสอบการดำเนินการ และตรวจสอบความเสี่ยง CloudAudit รองรับการดูบันทึกการดำเนินการของคอนโซล Tencent

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Cloud และ API คลาวด์ภายใน 90 วันออนไลน์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานและกลไกการรวบรวมและการจัดการบันทึก เพื่อควบคุมการบันทึก การดึงข้อมูล การจัดเก็บ การป้องกัน การวิเคราะห์ และการตรวจสอบบันทึกต่างๆ เช่น บันทึกการเข้าสู่ระบบ บันทึกการดำเนินการ บันทึกการระบบทั่วไป และบันทึกเหตุการณ์ความปลอดภัยของระบบ เพื่อตรวจจับและป้องกันความผิดปกติและความเสี่ยงของกิจกรรมระบบ บันทึกทั้งหมดถูกรวมเข้าสู่แพลตฟอร์มการจัดการบันทึกของ Tencent Cloud เพื่อการจัดการ และมีการใช้มาตรการสำรองข้อมูลและการป้องกันที่เข้มงวดสำหรับข้อมูลบันทึกที่เกี่ยวข้อง เพื่อป้องกันการแก้ไขและการลบโดยไม่ได้รับอนุญาต Tencent Cloud ดำเนินการตรวจสอบบันทึกผ่านเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติการและทีมตรวจสอบภายใน เพื่อตรวจจับความผิดปกติของระบบหรือการดำเนินการ เพื่อป้องกันความเสี่ยงในการปฏิบัติการ
4.2.3 (4)	การบริหารความ เสี่ยงด้านระบบ สารสนเทศ	(4.1)ปฏิบัติตามหลักเกณฑ์ของประกาศ ธปท. ว่าด้วยนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ เพื่อให้บริการการชำระเงินภายใต้การกำกับที่มีมาตรฐานในการบริหารความเสี่ยงด้านระบบสารสนเทศ มีความมั่นคงปลอดภัย (Security) มีความถูกต้องเชื่อถือได้ (Integrity) และมีความพร้อมในการให้บริการอย่างต่อเนื่อง (Availability) (4.2)จัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง และจัดทำรายงานผลการตรวจสอบเสนอต่อคณะกรรมการบริษัทหรือ	ลูกค้าควรให้มั่นใจว่าบริการชำระเงินของตนเป็นไปตามมาตรฐานการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) ดำเนินการตรวจสอบความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง รายงานการตรวจสอบต้องเสนอต่อคณะกรรมการหรือคณะกรรมการเพื่ออนุมัติ และต้องส่งสำเนารายงานการตรวจสอบต่อธนาคารแห่งประเทศไทยภายใน 45 วันนับจากวันที่การตรวจสอบเสร็จสิ้น เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเทศไทย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		อ คณะกรรมการที่ได้รับมอบหมายเพื่อพิจารณาให้ความเห็นชอบพร้อมส่งสำเนาผลการตรวจสอบให้ ธปท. เป็นหนังสือ หรือโดยวิธีการทางอิเล็กทรอนิกส์ตามที่กำหนด ภายใน 45 วันนับแต่วันทำการ ตรวจสอบแล้วเสร็จ โดยผู้ที่ทำหน้าที่ตรวจสอบดังกล่าวจะต้องมีความรู้ ประสบการณ์ และมีความเป็น อิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านความมั่นคงปลอดภัยทางระบบสารสนเทศ ทั้งนี้ ในกรณีที่ ธปท. เห็นว่าผลการตรวจสอบความมั่นคงปลอดภัย ทางระบบสารสนเทศ มีข้อมูลไม่ครบถ้วนหรือมีข้อความคลุมเครือไม่ชัดเจน หรือในกรณีที่ ธปท.ม เห็นว่าจำเป็นหรือสมควร ธปท. อาจสั่งให้ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับแต่งตั้ง ผู้ตรวจสอบภายนอกดำเนินการตรวจสอบและรายงานผลการตรวจสอบให้ ธปท.	ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบการจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็นอิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดเอกสารงานล่าสุดได้ด้วยตนเองจาก " Compliance Document Download "
4.2.3 (5)	รายอื่นหรือบุคคลอื่น	การใช้บริการจากบุคคลภายนอก กรณีผู้ประกอบการบริการการชำระเงินภายใต้การกำกับให้ผู้ให้บริการ รายอื่นหรือบุคคลอื่น (Outsourcing) มาดำเนินการแทนในงานระบบสารสนเทศ รวมถึงงานที่มีผลกระทบอย่างมีนัยสำคัญต่อธุรกิจบริการการชำระเงินภายใต้การกำกับ ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับยังคงมีความรับผิดชอบต่องานบริการในการให้บริการที่ต่อเนื่องปลอดภัย น่าเชื่อถือ	ลูกค้าที่ใช้ผู้ให้บริการภายนอกเพื่อจัดหาระบบเทคโนโลยีสารสนเทศสำหรับความต้องการในการดำเนินงานของตนเอง ควรสร้างกระบวนการจัดการความเสี่ยงเพื่อคัดเลือก ตรวจสอบ ประเมิน และทบทวนผู้ให้บริการภายนอก และทำข้อตกลงการจ้างทำภายนอกกับผู้ให้บริการภายนอก โดยกำหนดสิทธิในการตรวจสอบของตนให้ชัดเจน ลูกค้าควรจัดทำแผนความต่อเนื่องทางธุรกิจหรือแผนการกู้คืนจากภัยพิบัติ และทดสอบและอัปเดตแผนดังกล่าวเป็นประจำ นอกจากนี้ หากลูกค้าเลือกผู้ให้บริการภายนอกในต่างประเทศ ควรประเมินความเสี่ยง เช่น การส่งข้อมูลข้ามพรมแดน เป็นต้น

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		และความเสียหายใด ๆ ที่อาจเกิดขึ้น เสมือนกับเป็นการให้บริการโดยผู้ ประกอบธุรกิจเอง โดยผู้ประกอบธุรกิจบริการการช าระเงินภายใต้การกำกับต้องดำเนิน การ ดังต่อไปนี้ (5.1) จัดให้มีกระบวนการบริหารค วามเสี่ยง รวมทั้งการคัดเลือก ติดตาม ประเมินผล และตรวจสอบการให้บริการของผู้ ให้บริการรายอื่นหรือบุคคลอื่นอย างเหมาะสม โดย ประเมินความเสี่ยงของการใช้บริก การจากผู้ให้บริการรายอื่นหรือบุค คคลอื่นอย่างสม่ำเสมอ ทั้งนี้ ในการประเมินความเสี่ยง ควรครอบคลุมถึงความเสี่ยง ที่เกี่ยวข้องกับการรักษาความลับ และการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy) และผลกระทบ ต่อระบบงานที่สำคัญของผู้ประก อบธุรกิจบริการการชำระเงินภายใต้ การกำกับ (5.2) จัดให้มีการทำสัญญาการใช้ บริการ ซึ่งระบุสิทธิของผู้ตรวจสอบ ภายใน ผู้ตรวจสอบภายนอก และ ธปท. ในการเข้าตรวจสอบการดำเนินงาน และการควบคุมภายใน ของผู้ให้บริการรายอื่นหรือบุคคล อื่นในส่วนที่เกี่ยวข้องกับการประก อบธุรกิจบริการการชำระเงิน ภายใต้การกำกับนั้นได้ (5.3) จัดให้มีแผนรองรับการดำเนิน ธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) หรือแผนฉุกเฉินด้านเทคโนโลยีสา รสนเทศ (Disaster Recovery Plan) ที่ครอบคลุม	สำหรับการตรวจสอบอย่างละเอียด การประเมินความเสี่ยง หรือการทบทวนที่ลูกค้าขอ เมื่อลูกค้ายื่นคำร้อง Tencent Cloud จะให้ความร่วมมืออย่างแข็งขันในการจัดเตรียมข้อมูลให้แ กลูกค้า Tencent Cloud จะเจรจาตกลงกับลูกค้าตามสถานการณ์จริงและความต้อ งการของลูกค้าเพื่อกำหนดสิทธิในการตรวจสอบและสิทธิ ในการกำกับดูแลของลูกค้าในข้อตกลง สำหรับข้อตกลงการจ้างทำภายนอกที่กำกับลูกค้า Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์แบบเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสอง ฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้ ในด้านความต่อเนื่องทางธุรกิจของกิจกรรมการจ้ งทำภายนอก Tencent Cloud ได้ออกแบบและนำกรอบการจัดการความต่อเนื่องของธุ รกิจที่เหมาะสมกับสภาพแวดล้อมคอมพิวเตอร์คลาวด์ของ ตนเองไปใช้ และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจ Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภั ณฑ์และบริการคลาวด์ กำหนด RTO และ RPO ของแต่ละธุรกิจให้ชัดเจน และจัดทำกลยุทธ์การตอบสนองและแผนความต่อเนื่องขอ งธุรกิจที่แตกต่างกันตามผลการวิเคราะห์ผลกระทบทางธุ รกิจ รวมถึงจัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโด ยละเอียดสำหรับผลิตภัณฑ์คลาวด์ Tencent Cloud จะทำการทดสอบฝึกซ้อมความต่อเนื่องของธุรกิจสำหรับ ผลิตภัณฑ์คลาวด์เป็นประจำตามแผนความต่อเนื่องของธุ

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ถึงการใช้บริการจากผู้ให้บริการรายอื่นหรือบุคคลอื่น รวมทั้งต้องมีการทดสอบและทบทวนการปฏิบัติงานตามแผนอย่างสม่ำเสมอ เพื่อให้สามารถปฏิบัติงานได้จริง (5.4)กรณีที่มีการเลือกใช้บริการจากผู้ให้บริการรายอื่นหรือบุคคลอื่น ในต่างประเทศ โดยเฉพาะในด้านการจัดเก็บข้อมูล การประมวลผล หรือการดำเนินการใด ๆ เกี่ยวกับบน ข้อมูล ผู้ประกอบธุรกิจบริการการชำระเงินภายใต้การกำกับต้องมีการประเมินความเสี่ยงที่อาจเกิดขึ้นจากการใช้บริการในต่างประเทศนั้น เช่น ความเสี่ยงจากการไม่สามารถเข้าถึงข้อมูลอันเนื่องมาจากการขัดข้องหรือการปิดกั้นเครือข่ายสื่อสารหรือระบบสื่อสารระหว่างประเทศ (Information Access Risk) และความเสี่ยงด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติตามหลักเกณฑ์ของต่างประเทศ (Cross-border Compliance) และจัดให้มีแผนรองรับความเสี่ยงที่อาจเกิดขึ้น	ธุรกิจ เพื่อให้แน่ใจในความสามารถในการปฏิบัติได้จริงของแผนแผนฉุกเฉิน ฯลฯ สำหรับความเสี่ยงด้านข้ามพรมแดนที่อาจเกิดขึ้นจากการใช้บริการผู้ให้บริการบุคคลที่สาม โครงสร้างพื้นฐานของ Tencent Cloud ได้กระจายตัวอยู่ในหลายพื้นที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (zone) โดยแต่ละภูมิภาคเป็นพื้นที่ทางภูมิศาสตร์ที่แยกอิสระ และแต่ละโซนความพร้อมใช้งานเป็นโดเมนการบำรุงรักษา และรับมือเหตุขัดข้องที่แยกจากกัน โซนความพร้อมใช้งานแต่ละแห่งถูกแยกทางกายภาพ ลูกค้าสามารถวางระบบและจัดเก็บข้อมูลบนภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระตามความต้องการในการขยายธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อรับประกันความต้องการด้านการรับมือเหตุขัดข้องของธุรกิจ ภายในปี 2026 Tencent Cloud ได้ดำเนินการติดตั้งศูนย์ข้อมูลสามแห่งในประเทศไทย โดยมอบบริการคอมพิวเตอร์คลาวด์หลากหลายประเภท รวมถึงเซิร์ฟเวอร์คลาวด์ ฐานข้อมูลคลาวด์ และ CDN ลูกค้าชาวไทยสามารถเลือกเก็บและประมวลผลข้อมูลของตนในพื้นที่ประเทศไทยได้ Tencent Cloud ยึดมั่นในหลักการเปิดเผยและโปร่งใส โดยให้คำมั่นว่าลูกค้ามีสิทธิที่จะรับทราบข้อมูลเกี่ยวกับตำแหน่งการจัดเก็บข้อมูล รวมถึงตำแหน่งศูนย์ข้อมูลที่จัดเก็บข้อมูล สถานะการสำรองข้อมูลแบบเย็น (cold backup) และตำแหน่งการจัดเก็บข้อมูลสำรองแบบเย็น Tencent Cloud จะให้ข้อมูลเหล่านี้แก่ลูกค้าทางช่องทางที่เหมาะสมในเวลาอันสมควร Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด

10

Tencent Cloud จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทาง ระบบสารสนเทศ BOT อย่างไร

เพื่อกำหนดมาตรฐานนโยบายและมาตรการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่สำคัญ ระบบการชำระเงินที่กำหนด และบริการชำระเงินที่กำหนด ธนาคารแห่งประเทศไทยได้ออก [BOT No. SorNorChor 11/2561 เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ](#) และในภาคผนวกแนบปฏิบัติการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงิน ได้กำหนดกรอบนโยบายและมาตรการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างชัดเจน โดยใช้เป็นหลักการชี้แนะในการกำหนดขั้นตอนการตรวจสอบและมาตรการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่สำคัญ ระบบการชำระเงินที่กำหนด และบริการชำระเงินที่กำหนด ข้อกำหนดหลักครอบคลุมการควบคุมการเข้าถึงและการพิสูจน์ตัวตน ความลับของข้อมูลและความสมบูรณ์ของระบบ ความพร้อมใช้งานของระบบ การตรวจสอบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ และการทบทวนหรือปรับปรุงมาตรการความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ในบทนี้ Tencent Cloud จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จากนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ และภาคผนวกของมัน และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud จะช่วยสถาบันการเงินในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

10.1 เรื่อง

นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ- เนื้อหาหลัก

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
4.2.1	นโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศ	(1) ผู้ให้บริการหรือผู้ประกอบการจะต้องจัดทำนโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศเป็นลายลักษณ์อักษร โดยได้รับการพิจารณาอนุมัติจากคณะกรรมการ น. บริษัท ทั้งนี้ ผู้ให้บริการหรือผู้ประกอบการจะต้องเผยแพร่นโยบายดังกล่าวและอบรมให้แก่บุคลากรที่เกี่ยวข้องเพื่อถือปฏิบัติ รวมทั้งจัดให้มีการทบทวนหรือปรับปรุงนโยบายให้เหมาะสมกับสถานการณ์อย่างสม่ำเสมอ (2) นโยบายการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่มีความสำคัญ การให้บริการระบบการชำระเงินภายใต้	ลูกค้าควรกำหนดนโยบายความปลอดภัยเทคโนโลยีสารสนเทศ และได้รับอนุมัติจากคณะกรรมการ และสื่อสารนโยบายดังกล่าวไปยังพนักงานที่เกี่ยวข้อง จัดฝึกอบรมพนักงานเป็นประจำ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูล ซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยข้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดการความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ รวมถึงชี้แนะการทำงานประจำวันและกระบวนการจัดการของหน่วยงานและพนักงานทุกหน่วยในบริษัท นโยบายความปลอดภัยข้อมูลของ Tencent Cloud จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุมขั้นตอนการควบคุม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		การกำกับ และการให้ บริการการชำระเงินภายใต้การกำกับ แล้วแต่กรณี อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้	และมาตรการควบคุมของระบบการจัดการความปลอดภัย ภัยบนคลาวด์สอดคล้องกับนโยบายความปลอดภัย มาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบาย ความปลอดภัยข้อมูล
	(2.1) การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้		พนักงานสามารถดูนโยบายเหล่านี้ที่ Tencent Cloud เผยแพร่ผ่านแพลตฟอร์มภายในได้
	(2.2) การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ ของระบบสารสนเทศ		Tencent Cloud ยังได้สร้างกลไกการฝึกอบรมความปลอดภัยข้อมูลที่สม บูรณ์ภายในองค์กร โดยกำหนดให้พนักงานประจำ ที่ปรึกษา นักฝึกงาน และพนักงานภายนอก ต้องเรียนหลักสูตรฝึกอบรมความปลอดภัยข้อมูล
	(2.3) การรักษาสภาพความพร้อมใช้งาน ของการให้บริการ		หลักสูตรฝึกอบรมที่เกี่ยวข้องประกอบด้วยการฝึกอบรม บังคับสำหรับพนักงานทุกคน การฝึกอบรมเฉพาะทางสำหรับตำแหน่งงานสำคัญ และการฝึกอบรมวิชาชีพเลือกได้เอง เป็นต้น โดยเนื้อหาครอบคลุมด้านต่าง ๆ เช่น ความตระหนักด้านความปลอดภัยพื้นฐาน ความปลอดภัยในการทำงาน การระบุและป้องกันช่องโหว่
	(2.4) การตรวจสอบความมั่นคงปลอดภัย ทางระบบสารสนเทศ		การปกป้องความเป็นส่วนตัว การตอบสนองเหตุการณ์ มาตรฐานความปลอดภัยในการพัฒนา และข้อกำหนดด้านความปลอดภัยของข้อมูล Tencent Cloud มุ่งมั่นที่จะผนวกรวมการจัดการความปลอดภัยข้อมูลเข้า กับงานจัดการในชีวิตประจำวัน เพื่อให้มั่นใจว่าพนักงานเข้าใจและปฏิบัติตามนโยบายแ ละข้อกำหนดการจัดการความปลอดภัยข้อมูลภายใน นอกจากนี้ Tencent Cloud ยังได้รับใบรับรองและคุณวุฒิด้านความปลอดภัยและการ ปฏิบัติตามข้อกำหนดความเป็นส่วนตัวหลายรายการ เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, SOC ซึ่งพิสูจน์ว่าการจัดการความปลอดภัยและการสร้างการ ป้องกันข้อมูลส่วนบุคคลของ Tencent Cloud เป็นไปตามมาตรฐานการรับรองที่เกี่ยวข้องหรือแนวปฏิบัติ ที่ดีของอุตสาหกรรม และยังได้รับการตรวจสอบจากสถาบันตรวจสอบบุคคล ที่สามมืออาชีพเป็นประจำอีกด้วย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
4.2.2	มาตรการการ รักษาความม ั่นคงปลอดภัย ทางระบบสาร สนเทศ	มาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ผู้ให้บริการหรือผู้ประกอบการต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่มีความสำคัญ ระบบการชำระเงิน ภายใต้การกำกับ และบริการการชำระเงินภายใต้การกำกับ แล้วแต่กรณี ให้สอดคล้องกับนโยบาย ที่ได้กำหนดขึ้น และมาตรการดังกล่าวจะต้องเหมาะสมกับลักษณะของการให้บริการ โดยครอบคลุม ถึงการควบคุมการเข้าถึงและการพิสูจน์ตัวตนผู้ใช้ การรักษาความลับของข้อมูล การรักษาความถูกต้อง เชื่อถือได้ของระบบสารสนเทศ การรักษาสภาพความพร้อมใช้งานของการให้บริการ มีการแก้ไขปัญหา และการรายงาน รวมถึงจัดให้มีการตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง ตลอดจนจัดให้มีกระบวนการดูแลโดยคณะกรรมการบริษัทหรือผู้บริหารระดับสูง เพื่อให้มีการปฏิบัติตามมาตรการที่กำหนด ทั้งนี้ การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ ของผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ ผู้ประกอบการก็ระบบการชำระเงินภายใต้การกำกับ และผู้ประกอบการก็บริการการชำระเงินภายใต้การกำกับ ให้ปฏิบัติตามประกาศธนาคารแห่งประเทศไทย ที่เกี่ยวข้องกับหลักเกณฑ์การกำกับดูแล	ลูกค้าควรสร้างมาตรการความปลอดภัยระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงินที่สำคัญ ระบบการชำระเงินที่กำหนด หรือบริการชำระเงินที่กำหนด และกลไกการตรวจสอบเทคโนโลยีสารสนเทศ ดำเนินการตรวจสอบเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง และควรสร้างมาตรการเฝ้าระวังเพื่อให้แน่ใจว่ามาตรการความปลอดภัยได้รับการปฏิบัติตามอย่างมีประสิทธิภาพ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเทศไทย ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยภายในอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบ การจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็นอิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กร ที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการ ล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ไปด้วย นอกจากนี้ ผู้ให้บริการหรือผู้ประกอบการต้องดำเนินการทบทวนหรือ ปรับปรุงมาตรการตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบต่อกับนโยบาย และมาตรการที่ได้กำหนดไว้ ตลอดจนจัดอบรมและให้ความรู้แก่บุคลากรที่เกี่ยวข้อง	ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจาก " Compliance Document Download"

10.2

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศที่เกี่ยวข้องกับระบบการชำระเงิน

10.2.1 การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
1.1	การแบ่งแยกหน้าที่และความรับผิดชอบ	การกำหนดบุคลากรหรือหน่วยงานทางระบบสารสนเทศ และการแบ่งแยกอำนาจหน้าที่ที่เหมาะสมในการบริหารจัดการทางระบบสารสนเทศ ผู้ให้บริการหรือผู้ประกอบการต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากร หรือหน่วยงานที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางระบบสารสนเทศ รวมถึงสร้างความตระหนักให้ความรู้ และมีการอบรมให้กับบุคลากรภายในองค์กร ตลอดจนจัดให้มีกระบวนการทางวินัยเพื่อลงโทษ ในกรณีฝ่าฝืนหรือละเมิดระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัย	ลูกค้าควรมอบหมายบุคคลหรือหน่วยงานที่รับผิดชอบตามหลักการแบ่งแยกหน้าที่และความรับผิดชอบตามความจำเป็นในการจัดการระบบเทคโนโลยีสารสนเทศ และควรยกระดับจิตสำนึกด้านความปลอดภัยของพนักงาน และกำหนดบทลงโทษสำหรับพฤติกรรมที่ละเมิดระเบียบข้อบังคับด้านความปลอดภัย Cloud Access Management (CAM) สามารถช่วยลูกค้าจัดการการเข้าถึงผลิตภัณฑ์และบริการของ Tencent Cloud ได้อย่างปลอดภัยและละเอียดรอบคอบ โดยบัญชีผู้ใช้หลักจะได้รับสิทธิ์เข้าถึงทรัพยากรภายใต้ชื่อของตนโดยสมบูรณ์โดยอัตโนมัติ และสามารถสร้างผู้ใช้ย่อยและกำหนด ID ตัวตน ข้อมูลประจำตัว และสิทธิ์ให้กับผู้ใช้ย่อยได้ รองรับฟังก์ชันการตรวจสอบยืนยันตัวตนขั้นที่สองหลายวิธี รวมถึงการใช้การตรวจสอบโดยอุปกรณ์ MFA หรือการตรวจสอบด้วยรหัสยืนยันทางโทรศัพท์ เพื่อยืนยันความปลอดภัยของตัวตนและสภาพแวดล้อมก่อนเข้าสู่ระบบและดำเนินการที่ละเอียดอ่อน Tencent Cloud ยังได้กำหนดกลยุทธ์การอนุมัติสำหรับการควบคุมการเข้า

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ถึงและกลไกเมทริกซ์การแยกอำนาจภายในองค์กร โดยกำหนดให้บัญชีผู้ใช้ต้องใช้ตัวระบุเฉพาะ และตั้งค่านโยบายรหัสผ่านสำหรับบัญชีพนักงานตามแนว ทางความปลอดภัยขั้นพื้นฐาน ซึ่งรวมถึงความยาวรหัสผ่าน ความซับซ้อน การลือก และการรีเซต เป็นต้น สำหรับอุปกรณ์ปลายทาง ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายภายใน Tencent Cloud ได้กำหนดค่าการจำกัดจำนวนครั้งในการเข้าสู่ระบบที่ล้ม เหลวและนโยบายหมดเวลาการทำงานของเซสชัน Tencent Cloud ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการตรวจสอบสิทธิ์การเข้าถึงของพนักงาน โดยผู้ใช้ต้องผ่านการยืนยันตัวตนสองปัจจัยก่อนเข้าถึงท รพยากรภายใน Tencent Cloud ปฏิบัติตามหลักการสิทธิ์น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิ์น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิ์เฉพาะก็ต่อเมื่อมีความจำเป็นต้องใช้ และผ่านกระบวนการอนุมัติสิทธิ์ที่เข้มงวดเท่านั้น Tencent Cloud จะรักษามั่นทอนข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบ ทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดงานตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์ นอกจากนี้ Tencent Cloud ยังได้สร้างกลไกการฝึกอบรมความปลอดภัยข้อมูลที่สมบูรณ์ ภายในองค์กร โดยกำหนดให้พนักงานประจำ ที่ปรึกษา นักฝึกงาน และพนักงานภายนอก ต้องเรียนหลักสูตรฝึกอบรมความปลอดภัยข้อมูล และได้กำหนดประมวลการปฏิบัติสำหรับพนักงาน เพื่อควบคุมพฤติกรรมของพนักงาน กำหนดเกณฑ์การพิจารณาพฤติกรรมที่ละเมิดข้อกำหนด ความปลอดภัยข้อมูลและมาตรการจัดการและบทลงโทษ ที่สอดคล้องกันให้ชัดเจน
1.2	การควบคุมก ารเข้าถึงระบบ สารสนเทศ	ผู้ให้บริการหรือผู้ประกอบการธุรกิจต้อง จัดให้มีขั้นตอนปฏิบัติที่เป็นลายลักษณ์ อักษร สำหรับการควบคุม และจำกัดสิทธิ์การใช้ระบบสารสนเทศ ซึ่งเกี่ยวกับการให้บริการและข้อมูล ตาม ความจำเป็นในการใช้งาน	ลูกค้าควรใช้กลไกการจัดการควบคุมการเข้าถึง ควบคุมและจำกัดสิทธิ์การเข้าถึงสถานที่ อุปกรณ์ และระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการตาม ความต้องการ และบันทึกบัญชีการเข้าถึงและตรวจสอบเป็นประจำ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		เพื่อป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีความรู้ ทั้งจากภายในและ ภายนอกองค์กร	ในด้านการควบคุมการเข้าถึงทางกายภาพ Tencent Cloud ได้กำหนดขั้นตอนการเข้าถึงที่เป็นทางการสำหรับการเข้าถึงทางกายภาพของศูนย์ข้อมูล บุคคลที่ต้องการเข้าสู่ศูนย์ข้อมูลต้องแสดงตัวตนและนำหลักฐานแสดงตัวตนมายื่นต่อเจ้าหน้าที่ปฏิบัติการความปลอดภัย ผู้จัดการศูนย์ข้อมูลแต่ละแห่งต้องบันทึกและจัดการการมอบสิทธิ์ การแก้ไข และการยกเลิกสิทธิ์การเข้าถึงในระบบการเข้าถึงศูนย์ข้อมูลภายในของตน ผู้จัดการศูนย์ข้อมูลจะทบทวนสิทธิ์การเข้าถึงศูนย์ข้อมูลเป็นประจำ เพื่อให้มั่นใจว่ามีการจัดสรรสิทธิ์การเข้าถึงอย่างเหมาะสม หากสิทธิ์การเข้าถึงไม่เกี่ยวข้องหรือไม่จำเป็นอีกต่อไป ผู้จัดการศูนย์ข้อมูลของ Tencent Cloud จะปิดการใช้งานสิทธิ์การเข้าถึงดังกล่าว ผู้เยี่ยมชมที่ได้รับอนุมัติให้เข้าสู่ศูนย์ข้อมูลของ Tencent Cloud ล้วนได้รับการดูแลโดยวิศวกรภาคสนามของ Tencent Cloud ผู้เยี่ยมชมหรือพนักงานทุกประเภทที่เข้าออกศูนย์ข้อมูลต้องได้รับการตรวจสอบตัวตนและตรวจสอบสัมภาระที่พกพา และลงทะเบียนสิ่งของที่นำติดตัวมา ก่อนที่ผู้เยี่ยมชมจะเข้าสู่พื้นที่ศูนย์ข้อมูลและห้องเซิร์ฟเวอร์ ผู้จัดการศูนย์ข้อมูลต้องอนุมัติตัวตน วัตถุประสงค์ และระยะเวลาการเข้าชมของผู้เยี่ยมชม ผู้เยี่ยมชมที่ได้รับอนุมัติให้เข้าสู่ศูนย์ข้อมูล Tencent Cloud ล้วนได้รับการดูแลโดยวิศวกรภาคสนามของ Tencent Cloud และถูกตรวจสอบผ่านระบบวงจรปิดและแจ้งเตือน 24 ชั่วโมงของศูนย์ข้อมูล การเข้าถึงทางกายภาพในพื้นที่สำนักงานของ Tencent Cloud อยู่ภายใต้การควบคุมหลายระดับ รวมถึงการมีเจ้าหน้าที่รักษาความปลอดภัยประจำ การควบคุมด้วยบัตรผ่านประตู และการตรวจสอบด้วยระบบวงจรปิด (CCTV) นอกจากนี้ การเข้าสู่พื้นที่สำนักงานของ Tencent Cloud จำกัดเฉพาะบุคคลที่ได้รับการอนุมัติล่วงหน้าจากพนักงานภายในของ Tencent Cloud เท่านั้น ผู้เยี่ยมชมต้องลงทะเบียนที่จุดรักษาความปลอดภัยก่อนเข้า และแสดงเอกสารประจำตัวที่ถูกต้อง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และต้องได้รับอนุญาตจากพนักงานที่ได้รับมอบอำนาจเพื่อ เข้าสู่พื้นที่ กิจกรรมของผู้คนในพื้นที่สำนักงานของ Tencent Cloud ถูกบันทึกวิดีโอและตรวจสอบตลอด 24 ชั่วโมงผ่านระบบวงจรปิด (CCTV) ในด้านการควบคุมการเข้าถึงระบบ ลูกค้าสามารถใช้ <u>Cloud Access Management (CAM)</u> เพื่อมอบสิทธิ์การเข้าถึงทรัพยากรให้กับผู้ใช้ย่อยผ่านวิธีก ารต่างๆ เช่น แท็ก เพื่อให้บรรลุการควบคุมการเข้าถึงทรัพยากรคลาวด์อย่าง ละเอียด CAM ยังสนับสนุนการดูแลติดตามบันทึกการดำเนินการของพ นักงานผ่าน CloudAudit นอกจากนี้ Tencent Cloud ยังให้บริการ <u>Bastion Host (BH)</u> ที่สามารถสนับสนุนการอนุญาตอย่างละเอียดตามมิติต่าง ๆ เช่น ผู้ใช้ สิทธิ์ทรัพยากร บัญชีผู้ใช้ และสิทธิ์การดำเนินการ เพื่อให้มั่นใจว่าสิทธิ์ที่ผู้ใช้มีอยู่เป็นสิทธิ์ขั้นต่ำที่จำเป็นสำหรับ การเข้าถึงสิทธิ์และทำงานให้สำเร็จ เครื่องบินคัมกัน ยังสนับสนุนฟังก์ชันการตรวจสอบการดำเนินการ โดยบันทึกและวิเคราะห์บันทึกการดำเนินการของผู้ใช้ เพื่อให้มั่นใจว่าสามารถติดตามเหตุการณ์ความปลอดภัย ได้อย่างมีประสิทธิภาพ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ดูแล Tencent Cloud ยังได้กำหนดกลยุทธ์การให้สิทธิ์การควบคุมการเข้าถึงและ กลไกเมทริกซ์การแบ่งแยกสิทธิ์ภายในองค์กร Tencent Cloud ปฏิบัติตามหลักการสิทธิ์น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิ์น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิ์เฉพาะก็ต่อเมื่อมีความจำเป็นต้องใช้ และผ่านกระบวนการอนุมัติสิทธิ์ที่เข้มงวดเท่านั้น Tencent Cloud จะรักษานโยบายข้อมูลตัวตนของบุคลากรที่สอดคล้องกับ บทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดงานตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์ ประสงค์ สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้ เครื่องบินคัมกัน อย่างเต็มรูปแบบ โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบแ ปพลิเคชันจากส่วนกลางผ่าน เครื่องบินคัมกัน การเข้าถึง เครื่องบินคัมกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติสิทธิ์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			มีเฉพาะเจ้าหน้าที่ปฏิบัติการภายในของ Tencent Cloud บางส่วนเท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบ เครื่องบินคุ้มกัน ต้องการการยืนยันตัวตนสองปัจจัย บันทึกการดำเนินการปฏิบัติการจะถูกเก็บไว้โดยศูนย์กลางแพลตฟอร์มบันทึก (log) และได้รับการตรวจสอบโดยทีมตรวจสอบภายในของ Tencent Cloud เป็นประจำ
1.3	การตรวจสอบ ตัวตน และการป้องกัน การปฏิเสธ ความรับผิดชอบ	ผู้ให้บริการหรือผู้ประกอบการต้อง จัดให้มีการระบุ ตรวจสอบ หรือพิสูจน์ตัวตน และตรวจสอบสิทธิของผู้ใช้ระบบโด เมนพิจารณาใช้เทคโนโลยีที่เหมาะสม กับระดับความเสี่ยงของ ประเภทธุรกิจที่ให้บริการ เช่น การใช้รหัสผ่าน (Password) เลขประจำตัว (Personal Identification Number) อุปกรณ์หรือบัตรที่เก็บข้อมูลส่วนบุคคล (Token or Smart Card) ลักษณะทางชีวมาตร (Biometric) เทคโนโลยีกุญแจสาธารณะ (Public Key Infrastructure) เพื่อป้องกันการปฏิเสธ ความรับผิดชอบกรณีมีข้อพิพาทเกิดขึ้น	ลูกค้าควรใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมเพื่อควบคุม การเข้าถึงสินทรัพย์ข้อมูล และบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการปฏิเสธการกระทำ (repudiation) Cloud Access Management (CAM) สามารถช่วยลูกค้าจัดการการเข้าถึงผลิตภัณฑ์และทรัพยากร Tencent Cloud อย่างปลอดภัยและละเอียดรอบคอบ ผู้ใช้สามารถแก้ไขกฎรหัสผ่านของผู้ใช้ย่อยผ่านคอนโซล การจัดการการเข้าถึง รวมถึงความซับซ้อนของรหัสผ่าน ความยาว ระยะเวลาที่มีผล เป็นต้น เพื่อป้องกันไม่ให้รหัสผ่านรั่วไหล Tencent Cloud จะใช้การเข้ารหัสแฮช SHA256 และการเติมเกลือ (Salt) สำหรับรหัสผ่านของลูกค้า เพื่อหลีกเลี่ยงการเก็บรหัสผ่านในรูปแบบข้อความธรรมดา CAM ยังสนับสนุนฟังก์ชันการตรวจสอบยืนยันตัวตนขั้นที่สองท หลายวิธี รวมถึงการใช้การตรวจสอบโดยอุปกรณ์ MFA หรือการตรวจสอบด้วยรหัสยืนยันทางโทรศัพท์ เพื่อยืนยันความปลอดภัยของตัวตนและสภาพแวดล้อมก ่อนเข้าสู่ระบบและดำเนินการที่ละเอียดอ่อน Tencent Cloud ยังได้กำหนดกลยุทธ์การอนุมัติสำหรับการควบคุมการเข้า ถึงและกลไกเมทริกซ์การแยกอำนาจภายในองค์กร โดยกำหนดให้บัญชีผู้ใช้ต้องใช้ตัวระบุเฉพาะ และตั้งค่านโยบายรหัสผ่านสำหรับบัญชีพนักงานตามแนว ทางความปลอดภัยขั้นพื้นฐาน ซึ่งรวมถึงความยาวรหัสผ่าน ความซับซ้อน การลื และการรีเซ็ต เป็นต้น สำหรับอุปกรณ์ปลายทาง ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายภายใน Tencent Cloud ได้กำหนดค่าการจำกัดจำนวนครั้งในการเข้าสู่ระบบที่ล้ม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			หลายและนโยบายหมดเวลาการทำงานของเซสชัน Tencent Cloud ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการตรวจสอบสิทธิ์การเข้าถึงของพนักงาน โดยผู้ใช้อุปกรณ์ต้องผ่านการยืนยันตัวตนสองปัจจัยก่อนเข้าถึงทรัพยากรภายใน Tencent Cloud ปฏิบัติตามหลักการสิทธิ์น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิ์น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิ์เฉพาะก็ต่อเมื่อมีความจำเป็นต้องใช้ และผ่านกระบวนการอนุมัติสิทธิ์ที่เข้มงวดเท่านั้น Tencent Cloud จะรักษานโยบายข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดการตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์

10.2.2 การรักษาความลับของข้อมูล และความถูกต้องเชื่อถือได้ของระบบสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
2.1	การรักษาความลับ ของข้อมูล	ผู้ให้บริการหรือผู้ประกอบการธุรกิจ ต้องกำหนดขั้นตอน วิธีการในการรับส่ง ประมวลผล และการจัดเก็บข้อมูลอย่างเหมาะสม เพื่อรักษาความลับ ความถูกต้องสมบูรณ์ของข้อมูล	ลูกค้าควรกำหนดกลไกการปกป้องความปลอดภัยข้อมูล โดยจำแนกประเภทข้อมูลตามระดับความอ่อนไหวและความสำคัญ และดำเนินมาตรการป้องกันข้อมูลตามระดับข้อมูลที่แตกต่างกัน เพื่อให้มั่นใจว่ามีเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลระหว่างการส่งและข้อมูลที่จัดเก็บอยู่ในสถานะคงที่ได้ นอกจากนี้ ลูกค้าควรกำหนดกลไกในการลบไฟล์ลับและอุปกรณ์ทางกายภาพให้ชัดเจน เพื่อให้แน่ใจในความเป็นความลับและความสมบูรณ์ของข้อมูลลูกค้า ในด้านการป้องกันการจัดเก็บข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสานรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล Key Management Service (KMS) ใช้โมดูลความปลอดภัยฮาร์ดแวร์ (HSM) ที่ได้รับการรับรอง FIPS-140-2

ลำดับ ที่	โดเมนการคว บคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ในการสร้างและปกป้องคีย์ และสามารถสนับสนุนการจัดการวงจรชีวิตเต็มรูปแบบของ คีย์การเข้ารหัสของลูกค้า ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เน็ต Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มันก็มีประสิทธิภาพด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุ รกิจของลูกค้า นอกจากนี้ ลูกค้ายังสามารถใช้บริการ Tencent Cloud ต่อไปเพื่อให้บรรลุการถ่ายโอนข้อมูลที่ปลอดภัยในสถาน การณ์ต่างๆ: <u>Direct Connect (DC):</u> จัดเตรียมการเชื่อมต่อเครือข่ายแบนด์วิดท์สูงที่มีค วามเฉพาะตัวและความปลอดภัยสูง ผู้ใช้เป็นเจ้าของลิงก์เครือข่ายโดยเฉพาะ ไม่มีความเสี่ยงข้อมูลรั่วไหล <u>VPN Connection:</u> อิงตามเทคโนโลยีอุโมงค์เครือข่าย เพื่อให้บรรลุการถ่ายโอนข้อมูลที่ปลอดภัยระหว่างศ นย์ข้อมูลในพื้นที่และทรัพยากรบน Tencent Cloud อุโมงค์ VPN ใช้ IKE (โปรโตคอลแลกเปลี่ยนคีย์ลับ) และ IPsec เพื่อเข้ารหัสข้อมูลที่ถ่ายโอน สร้างอุโมงค์ข้อมูลที่ปลอดภัยและนำเชื่อถือบนอินเ ทอร์เน็ต เพื่อปกป้องความปลอดภัยของข้อมูลระหว่างการถ ายโอน สำหรับการลบและทำลายข้อมูล Tencent Cloud มีกลไกทำลายข้อมูลที่ปลอดภัยและเชื่อถือได้ เมื่อบริการของลูกค้าหมดอายุลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรอง อย่างสิ้นเชิงหลังช่วงเวลาเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้ เมื่อสื่อกู้ใช้ให้บริการ Tencent Cloud

ลำดับ ที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เกิดความขัดข้องและจำเป็นต้องเปลี่ยนหรือถึงอายุการใช้งานและจำเป็นต้องกำจัด Tencent Cloud จะลบข้อมูลที่เหลืออยู่ทันที และปฏิบัติตามขั้นตอนที่เข้มงวดเพื่อทำลายทางกายภาพอย่างสมบูรณ์ในเวลาที่เหมาะสม
2.2	การพัฒนาระบบ การควบคุมการเปลี่ยนแปลง การปรับปรุงแก้ไขระบบสารสนเทศหรืออุปกรณ์ประมวลผลสารสนเทศ	ผู้ให้บริการหรือผู้ประกอบการต้องกำหนดขั้นตอนปฏิบัติและการควบคุมภายในอย่างเป็นระบบสำหรับการพัฒนาและการควบคุมการเปลี่ยนแปลงหรือแก้ไขระบบสารสนเทศเพื่อลดความเสี่ยงที่จะทำให้ระบบที่ให้บริการเกิดความเสียหายหรือทำงานผิดปกติ	ลูกค้าควรใช้มาตรการควบคุมการพัฒนาระบบที่ปลอดภัยซึ่งครอบคลุมวงจรชีวิตทั้งหมดของการออกแบบ การพัฒนา การทดสอบ และการนำระบบไปใช้ และควรสร้างกลไกการจัดการการเปลี่ยนแปลงระบบโดยการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศควรได้รับการประเมิน ทดสอบ ตรวจสอบ และอนุมัติ ในด้านการจัดการการเปลี่ยนแปลง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานการจัดการสำหรับการเปลี่ยนแปลงผลิตภัณฑ์และการกำหนดค่าที่กำหนดขั้นตอนต่างๆ ในกระบวนการเปลี่ยนแปลงและผู้รับผิดชอบที่เกี่ยวข้องอย่างชัดเจน เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการอนุมัติและทดสอบอย่างเหมาะสมก่อนการดำเนินการ ในเวลาเดียวกัน Tencent Cloud ได้กำหนดขั้นตอนการจัดการสำหรับการเปลี่ยนแปลงฉุกเฉิน โดยการเปลี่ยนแปลงฉุกเฉินต้องได้รับการอนุมัติที่เหมาะสมก่อนจึงจะสามารถดำเนินการได้ การเปลี่ยนแปลงโปรแกรมทุกประเภท รวมถึงการเปลี่ยนแปลงแอปพลิเคชันและไฟล์กำหนดค่าระบบปฏิบัติการ และฐานข้อมูล ต้องได้รับการวิเคราะห์ผลกระทบทางธุรกิจก่อนการเปิดตัว จัดทำแผนย้อนกลับสำหรับการเปลี่ยนแปลง และได้รับการอนุมัติจากผู้รับผิดชอบที่เกี่ยวข้อง ระบบเผยแพร่การเปลี่ยนแปลงของ Tencent Cloud บังคับให้การดำเนินการเปลี่ยนแปลงสามารถดำเนินการได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น และเก็บรักษาบันทึกที่เกี่ยวข้องกับการเปลี่ยนแปลงไว้ พร้อมทั้งตรวจสอบบันทึกเป็นประจำ หลังการเผยแพร่การเปลี่ยนแปลง Tencent Cloud จะตรวจสอบ ตรวจสอบ และบันทึกผลการเปลี่ยนแปลงในสภาพแวดล้อมการผลิต Tencent Cloud

ลำดับ ที่	โดเมนการค บคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอการดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน และขอบเขตของการเปลี่ยนแปลง สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแวดล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม ในด้านการพัฒนาระบบ ลูกค้าสามารถใช้เครื่องมือพัฒนา Cloud-Native Build (CNB) ที่ Tencent Cloud ให้มา CNB ผสานแนวคิดการพัฒนายคล่องตัว (Agile) อย่างลึกซึ้ง ตั้งแต่ issue การรวมคำขอ ไปจนถึงชุดงานกระบวนการพัฒนายคล่องตัวได้รับการจัดตั้งขึ้นอย่างเป็นระเบียบ ช่วยลูกค้ายืนยันผลลัพธ์ของการเปิดตัวเวอร์ชันผลิตภัณฑ์สู่ตลาดด้วยงบประมาณที่ต่ำลงและวิธีการวนซ้ำที่เร็วขึ้น Tencent Cloud ยังได้สร้างมาตรฐานการพัฒนาความปลอดภัยระบบสารสนเทศภายในองค์กร และมุ่งมั่นผสานมาตรฐาน ISO/IEC 20000 การจัดการบริการเทคโนโลยีสารสนเทศ ระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001 และมาตรฐานระบบการจัดการคุณภาพ ISO/IEC 9001 เข้ากับกระบวนการวงจรชีวิตการพัฒนาความปลอดภัยผลิตภัณฑ์ทั้งหมด ให้ความสำคัญกับขั้นตอนต่างๆ เช่น ความต้องการ การออกแบบ การวิจัยและพัฒนา การทดสอบ การส่งมอบ และการดำเนินการและบำรุงรักษา ผสานแนวคิดด้านความปลอดภัยข้อมูลและการปกป้องความเป็นส่วนตัวเป็นส่วนตัวเข้าไปในแต่ละขั้นตอนของการพัฒนาผลิตภัณฑ์ เพื่อให้มั่นใจว่าผลิตภัณฑ์คลาวด์ได้รับความควบคุมด้านความปลอดภัยที่เพียงพอตลอดวงจรชีวิตของผลิตภัณฑ์ มาตรการควบคุมความปลอดภัยที่เกี่ยวข้อง ได้แก่: การฝึกอบรมความปลอดภัย: ส่งเสริมจิตสำนึกการเขียนโปรแกรมที่ปลอดภัยสำหรับนักพัฒนา กำหนดให้นักพัฒนาปฏิบัติตามมาตรฐานการเข้าร

ลำดับ ที่	โดเมนการคว บคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			รหัสที่ปลอดภัยอย่างเคร่งครัด การวิเคราะห์ความต้องการ: สื่อสารเกี่ยวกับเนื้อหาและกระบวนการธุรกิจ และกรอบทางเทคนิค เพื่อค้นหาวิธีที่ดีที่สุดในการฝังความปลอดภัย การออกแบบระบบ: สร้างแบบจำลองภัยคุกคามสำหรับการออกแบบระบบ และประเมินความปลอดภัยทางเทคนิคของสถาปัตยกรรมที่ใช้ การพัฒนาระบบ: ในระหว่างกระบวนการพัฒนา จัดเตรียมส่วนประกอบการพัฒนาความปลอดภัยที่ Tencent ออกแบบเองสำหรับนักพัฒนาใช้ และเขียนโค้ดตามมาตรฐานการเข้ารหัสความปลอดภัยของ Tencent Cloud การยืนยันความปลอดภัย: ค้นพบช่องโหว่ผ่านการตรวจสอบความปลอดภัยของโค้ด การสแกนความปลอดภัยของสินทรัพย์ การสแกนเว็บ การประเมินความปลอดภัยด้วยมนุษย์ การทดสอบเจาะระบบ และการตรวจสอบโค้ด การเผยแพร่: ระบบจะเผยแพร่ไปยังสภาพแวดล้อมออนไลน์ได้ก็ ต่อเมื่อความเสี่ยงสูงทั้งหมดได้รับการแก้ไขแล้ว เพื่อป้องกันไม่ให้เกิดผลกระทบทำงานในสภาพแวดล้อม การผลิตโดยมีช่องโหว่ด้านความปลอดภัย
2.3	การจัดการเครือข่ายที่เกี่ยวข้องกับการให้บริการ	ผู้ให้บริการหรือผู้ประกอบการธุรกิจ ต้องกำหนดมาตรการป้องกัน การเข้าถึงระบบ ที่ให้บริการทางเครือข่ายโดยไม่ ได้รับอนุญาต	ลูกค้าควรใช้มาตรการควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันไม่ให้อุปกรณ์ที่ไม่มีสิทธิ์เชื่อมต่อกับเครือข่าย ทบทวนกฎการควบคุมการเข้าถึงเครือข่ายเป็นประจำ และควรจัดการแบ่งส่วนเครือข่ายตามความสำคัญของระบบหรือความอ่อนไหวของข้อมูล และปรับใช้และติดตั้งอุปกรณ์ความปลอดภัยเครือข่าย สำหรับข้อกำหนดการแบ่งส่วนเครือข่าย ลูกค้าสามารถใช้บริการ Virtual Private Cloud (VPC) ที่ Tencent Cloud ให้มาเพื่อสร้างพื้นที่เครือข่ายอิสระหลายแห่งสำหรับทรัพยากรแพลตฟอร์มคลาวด์ที่ได้ซื้อไปแล้ว และกำหนดการแบ่งส่วนเครือข่ายและที่อยู่ IP นโยบายการกำหนดเส้นทาง ฯลฯ

ลำดับ ที่	โดเมนการคว บคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ตามต้องการได้ด้วยตนเอง บริการ VPC เป็นพื้นที่เครือข่ายบนคลาวด์เฉพาะที่สร้างขึ้นบน Tencent Cloud โดยเครือข่ายส่วนตัวใช้เทคโนโลยีโมงส์ สร้างเครือข่ายเสมือนบนเครือข่ายกายภาพ และใช้เทคโนโลยีเสมือนจริง เพื่อให้บรรลุการแยกอินเทอร์เน็ตโดยสมบูรณ์ระหว่างเครือ ข่ายส่วนตัวต่างๆ มอบเครือข่ายคลาวด์ที่ปลอดภัยเป็นอิสระและแยกจากกัน ให้กับลูกค้า สำหรับเซิร์ฟเวอร์คลาวด์ภายในเครือข่ายส่วนตัว สามารถควบคุมการไหลเข้าออกของข้อมูลในระดับอินสแ ตซ์และซับเน็ตได้ผ่านการกำหนดค่ากลุ่มความปลอดภัย และกฎ Access Control List (ACL) ของเครือข่าย เพื่อให้บรรลุการควบคุมการเข้าถึงเครือข่ายในระดับต่างๆ เพื่อดำเนินการป้องกันขอบเขตเครือข่าย Tencent Cloud ให้บริการ EdgeOne (EO) แก่ลูกค้า โดยอิงตามโหนดขอบทั่วโลกของ Tencent Cloud เพื่อมอบบริการป้องกันความปลอดภัยและเร่งความเร็วให้ กับลูกค้า มีฟังก์ชัน เช่น การป้องกัน DDoS การป้องกันเว็บอัจฉริยะ การป้องกันการโจมตีประเภทบอท/ครอว์เลอร์ การแก้ไข DNS และสนับสนุนให้ลูกค้าสามารถกำหนดกฎการควบคุมการ เข้าถึงแบบกำหนดเองตามความต้องการทางธุรกิจ <u>Cloud Firewall (CFW)</u> ให้การป้องกันขอบเขตเครือข่ายที่แตกต่างกันแก่ลูกค้าเป็น หลัก สนับสนุนการควบคุม ACL ของไฟร์วอลล์อย่างเข้มข้น การปิดกั้น IPS แบบเรียลไทม์ การปะชุดเสมือน และการตรวจจับภัยคุกคามที่เป็นอันตราย ฯลฯ สามารถตอบสนองความต้องการของโซน DMZ ในเครือข่ายแบบดั้งเดิม ปกป้องสินทรัพย์หลักเป็นพิเศษ และบรรลุการควบคุมการแยกอย่างละเอียดระหว่าง VPC <u>Web Application Firewall (WAF)</u> สามารถจัดการกับปัญหาความปลอดภัยของเว็บไซต์และ ธุรกิจเว็บ เช่น การโจมตีเว็บ การบุกรุก การใช้ประโยชน์จากช่องโหว่ การฝังมัลแวร์ การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต เบ็กดอร์ ครอว์เลอร์ ฯลฯ <u>Anti-DDoS</u> ใช้ทรัพยากรป้องกัน DDoS ที่มีคุณภาพและเพียงพอ ร่วมกับอัลกอริทึมการทำความสะอาดที่พัฒนาอย่างต่อเนื่อง อง "การพัฒนาด้วยตนเอง + การระบุอัจฉริยะด้วย AI"

ลำดับ ที่	โดเมนการคว บคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อจัดการกับปัญหาการโจมตี DDoS ในด้านความปลอดภัยในการสื่อสารเครือข่าย การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS VPN Connection ยังสามารถช่วยลูกค้าให้บรรลุการถ่ายโอนข้อมูลที่ปลอดภัยระหว่างศูนย์ข้อมูลในพื้นที่และทรัพยากรบน Tencent Cloud ภูมิภาค VPN ใช้ IKE (โปรโตคอลแลกเปลี่ยนคีย์ลับ) และ IPsec เพื่อเข้ารหัสข้อมูลที่ส่ง สร้างอุโมงค์ข้อมูลที่ปลอดภัยและนำเชื่อถือบนอินเทอร์เน็ต เพื่อป้องกันความปลอดภัยของข้อมูลระหว่างการส่ง สำหรับการแยกหลายผู้เช่า (Multi-tenancy Isolation) Tencent Cloud มีกลไกความปลอดภัย เช่น นโยบายการควบคุมการเข้าถึงทรัพยากรในชั้นควบคุมเสมือน (Virtualization Control Layer) นโยบายการแยกระหว่างเครือข่ายส่วนตัวภายในแพลตฟอร์มคลาวด์ การจัดสรรสิทธิ์และการยืนยันตัวตนบนเว็บคอนโซล รหัสเซสชันของอินเทอร์เน็ต และคีย์การเข้าถึง เพื่อให้มั่นใจว่าผู้ใช้แต่ละคนสามารถเข้าถึงทรัพยากรคอมพิวเตอร์คลาวด์ที่ตนซื้อได้เท่านั้น ซึ่งทำให้เกิดการแยกการเข้าถึงระหว่างผู้เช่าหลายรายได้อย่างมีประสิทธิภาพ ด้วยวิธีการแยกที่มีประสิทธิภาพ รับประกันว่าข้อมูลของลูกค้าในทรัพยากรเดียวกันไม่สามารถมองเห็นซึ่งกันและกัน รับประกันว่าผู้เช่าไม่สามารถเข้าถึง รับ หรือแก้ไขข้อมูลของผู้เช่าอื่นได้ ในการจัดการควบคุมความปลอดภัยเครือข่าย Tencent Cloud ยังได้สร้างมาตรฐานการจัดการความปลอดภัยเครือข่ายและระบบป้องกันเครือข่ายแบบหลายชั้นภายในองค์กร Tencent Cloud กำหนดมาตรฐานการควบคุมและป้องกันความปลอดภัยเครือข่าย ตลอดจนบทบาทและความรับผิดชอบที่เกี่ยวข้องอย่างชัดเจนผ่านระบบการจัดการและขั้นตอนการทำงาน เพื่อให้มั่นใจว่ากิจกรรมที่ดำเนินการบนเครือข่ายของ Tencent Cloud ดำเนินไปอย่างปลอดภัยในเวลาเดียวกัน Tencent Cloud ได้ปรับใช้สถาปัตยกรรมความปลอดภัยเครือข่ายที่ครบถ้วน

ลำดับ ที่	โดเมนการคว บคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			วน โดยใช้กลไกการป้องกันหลายชั้น เช่น ไฟร์วอลล์ ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) การป้องกัน DDoS การแยกทางลอจิกของเครือข่าย และความปลอดภัยของแอปพลิเคชันเว็บ เพื่อตรวจจับ กรอง และบล็อกการรับส่งข้อมูลเครือข่ายที่เป็นอันตรายได้ทันที ทังที่ ปกป้องความปลอดภัยเครือข่ายของ Tencent Cloud นอกจากนี้ Tencent Cloud ใช้มาตรการต่างๆ เช่น การควบคุมสิทธิ์และการอนุมัติขั้นตอน เพื่อห้ามไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงทรัพยากรเครือข่ายภายใน ซึ่งรวมถึงเครื่องมือวิเคราะห์และตรวจสอบเครือข่าย ในด้านการใช้และการควบคุมอุปกรณ์ความปลอดภัย กฎไฟร์วอลล์ของ Tencent Cloud ถูกกำหนดค่าให้จำกัดการเข้าถึงเครือข่ายการผลิตของ Tencent Cloud การเข้าถึงเพื่อจัดการกฎไฟร์วอลล์จำกัดเฉพาะผู้จัดการที่ ได้รับอนุญาตที่ใช้การยืนยันตัวตนสองปัจจัยเท่านั้น สำหรับการทบทวนเป็นประจำเกี่ยวกับสถาปัตยกรรมความ ปลอดภัยเครือข่ายและกลยุทธ์การป้องกัน ทีมเครือข่ายของ Tencent Cloud จะทบทวนการออกแบบความปลอดภัยและสถานะการเชื่อม ต่อของระบบเครือข่าย การกำหนดค่าของระบบป้องกัน (รวมถึงไฟร์วอลล์, IPS/IDS, การป้องกัน DDoS เป็นต้น) อย่างครอบคลุมเป็นประจำ เพื่อระบุช่องโหว่ด้านความปลอดภัยและอัปเดตกฎการป้อ งกันความปลอดภัยได้ทันที การเปลี่ยนแปลงทั้งหมดที่เกี่ยวข้องกับสถาปัตยกรรมเครี ข่ายและอุปกรณ์ต้องปฏิบัติตามขั้นตอนการจัดการการเ ปลี่ยนแปลงที่เข้มงวด ดำเนินการอย่างเป็นมาตรฐานหลังจากเสร็จสิ้นการวิเคราะห์ ผลกระทบของการเปลี่ยนแปลง จัดทำแผนย้อนกลับ และได้รับอนุมัติและการอนุญาตที่เหมาะสม

10.2.3 การรักษาสภาพความพร้อมใช้งานของการให้บริการ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
3.1	การประเมิน และจัดการคว ามเสี่ยงของระ บบที่ให้บริการ	ผู้ให้บริการหรือผู้ประกอบการต้อง มีวิธีการประเมินความเสี่ยงของระบบ ที่ให้บริการ ที่เหมาะสม กำหนดเกณฑ์ในการยอมรับความเ ี่ยงและระบุระดับความเสี่ยงที่ยอมรับ ได้ รวมถึงกำหนด วิธีการจัดการความเสี่ยงที่อาจเกิดขึ้ น ทั้งนี้ผู้ให้บริการและผู้ประกอบการ ต้องจัดให้มีการทบทวน ความเสี่ยงอยู่เสมอ ให้สอดคล้องกับพัฒนาการทางเทคโนโลยีและสถานการณ์ปัจจุบัน	ลูกค้าควรกำหนดวิธีการประเมินความเสี่ยง ดำเนินการตรวจสอบความเสี่ยงเป็นประจำ กำหนดความชอบและระดับความอดทนต่อความเสี่ยง (risk appetite and risk tolerance) ให้ชัดเจน และจัดทำและดำเนินการตอบสนองต่อความเสี่ยงสำ หรับความเสี่ยงที่ระบุได้ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ดูแล Tencent Cloud ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัย ภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามงานต่างๆ เช่น การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยงไว้อย่างชัดเจน Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุความเสี่ยงตามสถานการณ์ความเสี่ยง ผลิตภัณฑ์ทางธุรกิจ หรือกระบวนการให้บริการ สำหรับความเสี่ยงที่ระบุได้ Tencent Cloud จะประเมินความเป็นไปได้และระดับผลกระทบของความเสี่ยง แต่ละรายการเพื่อจำแนกระดับความเสี่ยง และดำเนินการตามขั้นตอนที่สอดคล้องกันต่อไป โดยมีการบันทึกกิจกรรมกระบวนการทั้งหมดไว้ Tencent Cloud ยังติดตามสถานการณ์การจัดการความเสี่ยงอย่างต่อเนื่อง ประเมินความเสี่ยงที่เหลืออยู่ และมั่นใจว่าผู้เกี่ยวข้องได้จัดการความเสี่ยงอย่างเหมาะสม ตามข้อกำหนดการจัดการความเสี่ยงของ Tencent Cloud นอกจากนี้ Tencent Cloud บำรุงรักษาและปรับปรุงวิธีการประเมินความเสี่ยงและเพิ่ ย่นความเสี่ยงอย่างต่อเนื่องตามแนวโน้มการเปลี่ยนแปลงใ นอุตสาหกรรมคลาวด์และแนวปฏิบัติการจัดการภายใน
		ผู้ให้บริการหรือผู้ประกอบการต้อง กำหนดให้มีการติดตาม ตรวจสอบความผิดปกติ ตลอดจนข้อมูลข่าวสารที่เกี่ยวข้องกับช องโหว่ในระบบต่าง ๆ ที่ให้บริการ เพื่อประเมินความเสี่ยงและ กำหนดมาตรการรองรับเพื่อลดควา มเสี่ยงดังกล่าว	ลูกค้าควรเฝ้าระวังและตรวจจับภัยคุกคามหรือพฤติกรรม การเข้าถึงโดยไม่ได้รับอนุญาตต่อระบบเทคโนโลยีสารสนเทศ และประเมินและซ่อมแซมช่องโหว่ของระบบเป็นประจำ โดยเฉพาะอย่างยิ่งสำหรับระบบที่มีความเสี่ยงสูง ควรดำเนินการทดสอบเจาะระบบ (penetration testing) เพื่อตรวจสอบประสิทธิภาพของเทคโนโลยีความปลอดภัย ในด้านการตรวจจับภัยคุกคาม เพื่อสนับสนุนลูกค้าในการตรวจจับและวิเคราะห์ภัยคุกคาม Tencent Cloud ให้บริการ Threat Intelligence

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			X (TIX) แก่ลูกค้า ซึ่งเป็นแพลตฟอร์มบริการข่าวกรองแบบครบวงจร TIX สามารถให้ความสามารถด้านข่าวกรองสามประเภทหลัก ได้แก่ ข่าวกรองพื้นฐาน ข่าวกรองด้านพื้นผิวการโจมตี และข่าวกรองทางธุรกิจ รองรับฟังก์ชันต่างๆ เช่น การสืบค้นข่าวกรอง การวิเคราะห์และประเมิน IOC การจัดการพื้นผิวการโจมตี สามารถช่วยลูกค้าวิเคราะห์และประเมินเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น และประเมินความเสี่ยงด้านการเปิดเผยสินทรัพย์ขององค์กรอย่างครอบคลุมมากขึ้น สนับสนุนองค์กรในการสร้างระบบป้องกันความปลอดภัยแบบสามมิติที่มีประสิทธิภาพ TIX สร้างเครือข่ายจุดสัมผัสข่าวกรองที่สมบูรณ์ โดยรวบรวมและวิเคราะห์ข่าวกรองภัยคุกคามจากแหล่งที่มาหลากหลาย เช่น ชุมชนช่องโหว่ องค์กรความปลอดภัย ผู้ผลิตเครื่องมือความปลอดภัย โซเชียลมีเดีย บล็อกความปลอดภัย และเชื่อมโยงกับอัลกอริธึมและพลังการคำนวณบนคลาวด์ เพื่อจัดผลบวกปลอม ซึ่งรับประกันความแม่นยำของข่าวกรอง นอกจากนี้ ศูนย์ข่าวกรองภัยคุกคามใช้ SaaS เป็นแกนกลาง รองรับวิธีการส่งมอบต่างๆ เช่น API ผังเว็บ SDK TIP และ Mini Program เพื่อตอบสนองความต้องการที่หลากหลายของลูกค้า ศูนย์ข่าวกรองภัยคุกคามยังสามารถบูรณาการกับผลิตภัณฑ์ป้องกันความปลอดภัยที่มีอยู่ของลูกค้าในรูปแบบการรวมเข้าด้วยกัน เพื่อเชื่อมโยงข้อมูลข่าวกรองจากคลาวด์กับผลิตภัณฑ์ดังกล่าว เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัยโดยรวมและการตอบสนองต่อภัยคุกคาม ด้วยการเสริมพลังและการสนับสนุนจากศูนย์ข่าวกรองภัยคุกคาม Tencent Cloud มุ่งมั่นที่จะสร้างระบบความสามารถด้านความปลอดภัยในการป้องกันเชิงรุกแบบ "ข่าวกรอง-การโจมตีและการป้องกัน-การจัดการ-การวางแผน" โดยบูรณาการเทคโนโลยีต่างๆ เช่น ข่าวกรองภัยคุกคาม ปัญญาประดิษฐ์ ข้อมูลขนาดใหญ่ เพื่อเพิ่มความสามารถและประสิทธิภาพในการตอบสนองต่อเหตุการณ์ความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และได้จัดตั้งศูนย์ปฏิบัติการความปลอดภัยที่ทำงาน 24 ชั่วโมงทุกวัน ให้ความสำคัญกับการตรวจจับภัยคุกคาม การสอบสวน และการตอบสนอง เพื่อให้บรรลุความสามารถในการรับรู้มองเห็น และควบคุมสถานการณ์ความปลอดภัย ในการเฝ้าระวังความปลอดภัยของระบบที่ผิดปกติ Tencent Cloud ให้บริการ Cloud Log Service (CLS) ซึ่งเป็นแพลตฟอร์มบริการบันทึกแบบครบวงจร CLS ให้บริการหลายรายการตั้งแต่การรวบรวมบันทึก การจัดเก็บบันทึก ไปจนถึงการสืบค้นและวิเคราะห์บันทึก การบริโภคแบบเรียลไทม์ และการส่งบันทึก ช่วยลูกค้าแก้ไขปัญหาต่างๆ เช่น การดำเนินงานทางธุรกิจ การตรวจสอบความปลอดภัย การตรวจสอบบันทึก และการวิเคราะห์บันทึก Cloud Security Center (CSC) ยังสนับสนุนการรวบรวมข้อมูลที่เกี่ยวข้องกับความปลอดภัยบนคลาวด์ประเภทต่างๆ เช่น ข้อมูลการแจ้งเตือนของผลิตภัณฑ์ความปลอดภัยคลาวด์ ข้อมูลการเปลี่ยนแปลงการกำหนดค่าสินทรัพย์คลาวด์ ข้อมูลพฤติกรรมกรรมการดำเนินการของผู้ใช้บนคลาวด์ และข้อมูลบันทึกของผลิตภัณฑ์คลาวด์บางส่วน และให้แพลตฟอร์มการสืบค้นและสอบสวนแบบครบวงจร ช่วยลูกค้าบรรลุการตรวจสอบบันทึกและการสืบค้นและสอบสวนบันทึกบนคลาวด์อย่างครอบคลุม นอกจากนี้ บริการ Elasticsearch Service (ES) จะรวบรวมและส่งบันทึกแบบเรียลไทม์ของเซิร์ฟเวอร์คลาวด์ คอนเทนเนอร์ และผลิตภัณฑ์คลาวด์อื่นๆ หรือข้อมูลธุรกิจที่มีอยู่และเพิ่มขึ้นของธุรกิจไปยังคลัสเตอร์ ES ของ Tencent Cloud เพื่อจัดเก็บข้อมูลแบบกระจาย และการสืบค้นและการวิเคราะห์ข้อมูล ภายใน Tencent Cloud ได้สร้างมาตรฐานและกลไกการรวบรวมและการจัดการบันทึก เพื่อควบคุมการบันทึก การดึงข้อมูล การวิเคราะห์ และการตรวจสอบข้อมูลบันทึกต่างๆ เช่น บันทึกการเข้าสู่ระบบ บันทึกการดำเนินการ และบันทึกเหตุการณ์ เพื่อตรวจจับและป้องกันความผิดปกติและความเสี่ยงของกิจกรรมระบบ Tencent Cloud ยังติดตั้งระบบตรวจสอบเครือข่ายภายในเพื่อตรวจสอบและแจ้งเตือนอุปกรณ์เครือข่าย เช่น เราเตอร์ไฟร์วอลล์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และเซิร์ฟเวอร์เครือข่าย และติดตามและแก้ไขปัญหาด้านความปลอดภัยที่ตรวจพบผ่านระบบภายใน เวลาเดียวกัน Tencent Cloud กำหนด "เส้นแดง" ความปลอดภัยในการปฏิบัติงานโดยละเอียด และด้วยประสบการณ์ที่สะสมมาหลายปีในการตรวจสอบพฤติกรรมที่ผิดปกติ ได้สร้างฐานข้อมูลกฎที่สมบูรณ์และพัฒนาเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติงานที่เชื่อถือได้ ซึ่งสามารถระบุพฤติกรรมที่ผิดปกติและทริกเกอร์การแจ้งเตือนแบบเรียลไทม์โดยอัตโนมัติได้อย่างทันท่วงที ในด้านการดำเนินกิจกรรมการสแกนช่องโหว่และการทดสอบเจาะระบบ Tencent Cloud ให้บริการ <u>Penetration Testing Service (PTS)</u> แก่ลูกค้าด้วยการจำลองเทคนิคการโจมตีและเทคนิคการค้นพบช่องโหว่ที่แฮกเกอร์อาจใช้อย่างเต็มรูปแบบ ใช้วิธีการและกลไกที่ควบคุมได้และไม่ทำลายล้างเพื่อทำการตรวจสอบความปลอดภัยของระบบเป้าหมายอย่างลึกซึ้ง ค้นหาจุดอ่อนที่มีอยู่ในเป้าหมายและอุปกรณ์เครือข่าย ให้คำแนะนำในการเสริมความแข็งแกร่งด้านความปลอดภัยเพื่อช่วยลูกค้ายกระดับความปลอดภัยของระบบ และสนับสนุนการตรวจสอบหลังการแก้ไขช่องโหว่ ในด้านการสแกนช่องโหว่ ลูกค้าสามารถเลือกใช้ <u>Vulnerability Scanning Service (VSS)</u> เพื่อตรวจสอบสินทรัพย์เครือข่ายขององค์กรและระบุความเสียหายของสินทรัพย์นั้นๆ โดยใช้ประโยชน์จากประสบการณ์ด้านความปลอดภัยและข่าวกรองภัยคุกคามที่สะสมมาหลายปีของ Tencent Cloud VSS ได้สร้างฐานข้อมูลกฎช่องโหว่ที่อุดมสมบูรณ์และครอบคลุม และมีความสามารถในการตรวจจับช่องโหว่ 0Day/1Day/NDay ที่มีอาชีพและมีประสิทธิภาพสูง สามารถดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของสินทรัพย์ของลูกค้า ให้คำแนะนำการแก้ไขที่มีอาชีพแก่ลูกค้า เพื่อลดความเสี่ยงด้านความปลอดภัย VSS ยังสนับสนุนการทำงานร่วมกับผลิตภัณฑ์คลาวด์ เช่น ความปลอดภัยโฮสต์ ไฟร์วอลล์แอปพลิเคชันเว็บ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อให้บรรลุวงจรปิดจากการตรวจสอบความเสี่ยงไปจนถึงการจัดการความเสี่ยง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะสร้างงานสแกนเป็นประจำผ่านระบบสแกนช่องโหว่เพื่อสแกนช่องโหว่ของสินทรัพย์ในสภาพแวดล้อมคลาวด์และวิเคราะห์ จัดประเภท และดำเนินการแก้ไขช่องโหว่ที่พบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะดำเนินการทดสอบเจาะระบบขนาดใหญ่แบบเต็มวงจรเป็นประจำ และดำเนินการทดสอบเจาะระบบแบบเจาะจงอย่างยืดหยุ่นในสถานการณ์ต่างๆ เช่น ก่อนการเปิดตัวผลิตภัณฑ์ใหม่หรือเมื่อมีการเปลี่ยนแปลงครั้งสำคัญ ผลการทดสอบเจาะระบบจะแจ้งให้ฝ่ายงานผู้รับผิดชอบที่เกี่ยวข้องทราบผ่านใบงานความปลอดภัย และฝ่ายงานผู้รับผิดชอบจะดำเนินการปะช่องโหว่หรือดำเนินการมาตรการควบคุมชนิดอื่นๆ ทันที เพื่อให้มั่นใจว่าช่องโหว่ที่ใช้ประโยชน์ได้ซึ่งพบในการทดสอบเจาะระบบได้รับการจัดการอย่างเหมาะสม นอกจากนี้ Tencent Cloud ยังดำเนินการฝึกซ้อมการต่อสู้เสมือนระหว่างทีมแดงและทีมน้ำเงินเพื่อจำลองการต้านทานการโจมตีทางเครือข่ายเป็นประจำ Tencent Cloud ยังได้สร้างแพลตฟอร์มรับข้อเสนอแนะช่องโหว่จากภายนอกและดำเนิน "โครงการให้รางวัลการรายงานช่องโหว่" โดยเชิญผู้เชี่ยวชาญด้านความปลอดภัยในอุตสาหกรรมช่วย Tencent Cloud ค้นพบช่องโหว่และความเสี่ยงด้านความปลอดภัยของระบบจากมุมมองของแฮกเกอร์ เพื่อแก้ไขปัญหาด้านความปลอดภัยได้ทันเวลาที่และบำรุงรักษาความปลอดภัยของระบบนิเวศของ Tencent Cloud
3.3	การแก้ไขปัญหา บันทึกเหตุการณ์ และการรายงาน	ผู้ให้บริการหรือผู้ประกอบการต้องมีการติดตาม บันทึก และรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยผ่านช่องทางการรายงานที่กำหนดไว้ โดยดำเนินการอย่างรวดเร็วที่สุด	ลูกค้าควรสร้างกลไกการตอบสนอง การจัดการ การบันทึก และการรายงานเหตุการณ์ความปลอดภัยเพื่อเฝ้าระวังและบันทึกเหตุการณ์ความปลอดภัยที่เกิดขึ้นและสรุปบทเรียนจากประสบการณ์ในอดีต ในด้านการตรวจจับและตอบสนองต่อเหตุการณ์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดความเฉพาะ	การตอบสนองของ Tencent Cloud
	กรณีระบบสา รสนเทศได้รับ ความเสียหาย	เท่าที่จะทำได้ รวมทั้งให้มีการเรียนรู้จากเหตุการณ์ ที่เกิดขึ้นแล้ว เพื่อเตรียมการป้องกันที่จำเป็น ไว้ล่วงหน้า	Tencent Cloud ได้สร้างขั้นตอนการจัดการเหตุการณ์โดยละเอียด โดยใช้ระบบการดำเนินงานความปลอดภัยภายในเพื่อบัน ทึกเหตุการณ์ความปลอดภัย สำหรับเหตุการณ์ความปลอดภัยที่ตรวจจับและระบุได้ Tencent Cloud จะวิเคราะห์และจำแนกระดับเหตุการณ์โดยพิจารณาจาก ปัจจัยต่างๆ เช่น ลักษณะของเหตุการณ์ ระดับความอ่อนไหวของข้อมูล และขอบเขตของผลกระทบ และจะแจ้งให้ผู้รับผิดชอบที่เกี่ยวข้องทราบทันทีเพื่อดำเน ิการจัดการเหตุการณ์ ที่มุ่งความปลอดภัยของ Tencent Cloud ได้สร้างกลไกการวิเคราะห์เหตุการณ์เป็นระยะ โดยจะวิเคราะห์เหตุการณ์หลายมิติเป็นประจำ (ประเภทเหตุการณ์ ความถี่ในการเกิด ขอบเขตผลกระทบ และระดับความรุนแรง) และดำเนินมาตรการป้องกันตามการทบทวนเหตุการณ์แ ละการวิเคราะห์สาเหตุรากฐาน เพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่คล้ายคลึงกันเกิดขึ้นอีก สำหรับเหตุการณ์ความปลอดภัยที่สำคัญ Tencent Cloud จะจัดตั้งทีมเฉพาะกิจเพื่อจัดทำรายงานการวิเคราะห์เฉพาะ เรื่องเสนอต่อฝ่ายบริหาร ในด้านการสื่อสารและการแจ้งเหตุการณ์ Tencent Cloud ได้กำหนดมาตรฐานการจัดการเหตุการณ์ความปลอดภัย ข้อมูล สร้างขั้นตอนที่เกี่ยวข้อง เช่น การตอบสนองเหตุการณ์ความปลอดภัยข้อมูล การยกระดับเหตุการณ์ และการแจ้งเหตุการณ์ เพื่อแจ้งเตือนหรือแจ้งให้พนักงานภายในบริษัท ลูกค้า และผู้เกี่ยวข้องอื่น ๆ ที่อาจหรือได้รับผลกระทบจากอุบัติเหตุทราบทันเวลา ทำให้ทุกฝ่ายสามารถสื่อสารและประสานงานกันอย่างเป็น ระเบียบ ทันเวลา และมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบ ต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ค วามปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้ เหลือน้อยที่สุด ในด้านการที่ลูกค้าแจ้งปัญหาหรือติดต่อ Tencent Cloud คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการในงาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับ ระบบในงานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับในงานของลูกค้าผ่านกลไก การตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมและจั ดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้าไ ด้รับการตอบสนองและจัดการอย่างทันทั่วทั้ง นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเป็ นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พบ เมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้าไ ด้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเวลา ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับการส สนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า
3.4	การสำรองข้อ มูล	ผู้ให้บริการหรือผู้ประกอบการธุรกิจต้อง จัดให้มีการสำรองและทดสอบข้อมูล ที่สำรอง เก็บไว้อย่างสม่ำเสมอ เพื่อรักษาความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้งานของการ ให้บริการ	ลูกค้าควรสร้างกลไกการจัดการการสำรองข้อมูล ทำการสำรองข้อมูลสำหรับข้อมูลลับและข้อมูลที่ละเอียดว่ อน และเข้ารหัสและปกป้องทางกายภาพสำหรับสื่อจัดเก็บข้อ มูลสำรอง และดำเนินการทดสอบการกู้คืนจากการสำรองข้อมูลเป็น ประจำ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Tencent Cloud ให้มาส่วนนี้ฟังก์ชันการสำรองข้อมูลเพื่อตอบสนองความต้องการสำรองข้อมูลทุกประเภทของลูกค้า ตัวอย่างเช่น: ข้อมูลที่ลูกค้าเก็บไว้ใน Cloud Object Storage (COS) สามารถจัดเก็บข้อมูลในหลายพื้นที่ที่กำหนดพร้อมกันได้ผ่านฟังก์ชันการทำสำเนาข้ามพื้นที่เพื่อให้แน่ใจว่าแม้ในกรณีที่สูญหายข้อมูลบางส่วนไปโดยไม่ได้อาการหมาย ก็สามารถค้นหาและกู้คืนข้อมูลทั้งหมดได้ผ่านข้อมูลสำรอง และยังหลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้นเมื่อพื้นที่เก็บข้อมูลในโซนความพร้อมใช้งานหนึ่งประสบภัยพิบัติที่ไม่อาจหลีกเลี่ยงได้ ซึ่งช่วยให้บรรลุผลสำรองข้อมูลหลายชุดและการกู้คืนจากภัยพิบัติข้ามพื้นที่ ฟังก์ชันการสำรองข้อมูลแบบสแนปช็อตของ Cloud Block Storage (CBS) ทำการสำรองข้อมูลโดยการถ่ายสแนปช็อต ณ จุดเวลาใดเวลาหนึ่งของ CBS ป้องกันการสูญหายข้อมูลเนื่องจากการแก้ไขโดยไม่ได้รับอนุญาตและการลบผิดพลาด และรับประกันความสามารถในการย้อนกลับอย่างรวดเร็วเมื่อเกิดความขัดข้องทางธุรกิจ Cloud File Storage (CFS) ให้ฟังก์ชันสแนปช็อตเป็นระยะ เพื่อความสะดวกในการตั้งค่านโยบายงานสำรองข้อมูลตามความยืดหยุ่นของลูกค้า Cloud Native Database TDSQL-C รองรับการสำรองข้อมูลสองประเภท: การสำรองข้อมูลเชิงตรรกะและการสำรองข้อมูลแบบสแนปช็อต ด้วยการสำรองข้อมูลที่สมบูรณ์และการสำรองข้อมูล binlog ในช่วงเวลาต่อมา ทำให้สามารถกู้คืนคลัสเตอร์ TDSQL-C MySQL Edition ทั้งหมดหรือตารางฐานข้อมูลเฉพาะไปยังจุดเวลาใดก็ได้ TencentDB for MySQL รองรับสองวิธีในการสำรองข้อมูลฐานข้อมูล:

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
3.5	การจัดทำแผน รองรับการ ดำเนินธุรกิจ อย่างต่อเนื่อง หรือแผนฉุกเฉินทางระบบ สารสนเทศ	ผู้ให้บริการหรือผู้ประกอบการต้อง จัดทำแผนสร้างความต่อเนื่องให้กับ การให้บริการ ระบบการชำระเงินที่มีความสำคัญ ระบบการชำระเงินภายใต้การกำกับ หรือบริการการชำระเงินภายใต้ การกำกับ แล้วแต่กรณี และนำแผนมาดำเนินการเพื่อให้บริ การสามารถดำเนินต่อไปได้ตามระยะ เวลา ที่กำหนดไว้หลังจากที่มีเหตุการณ์ที่ ทำให้บริการหยุดชะงัก	การสำรองข้อมูลอัตโนมัติและการสำรองข้อมูลด้วย ตนเอง และให้ฟังก์ชันการสำรองข้อมูลข้ามพื้นที่ เพื่อช่วยลูกค้าเพิ่มความสามารถในการกู้คืนจากภัย พิบัติและเพิ่มความน่าเชื่อถือของข้อมูลไปพร้อมๆ กัน TencentDB for MongoDB ให้กลไกการสำรองข้อมูลอัตโนมัติและการกู้คืนโดยไ มสูญเสียข้อมูล รองรับการสำรองข้อมูลแบบหลายโหนด ลูกค้าสามารถเก็บข้อมูลสำรองไว้หลายวันผ่านกลไ กการสำรองข้อมูล เพื่อความสะดวกในการกู้คืนข้อมูลในสถานการณ์กั ยพิบัติ
			ลูกค้าวิเคราะห์และระบุขั้นตอนสำคัญของธุรกิจ จัดทำแผนความต่อเนื่องทางธุรกิจ กำหนดเป้าหมายเวลาในการกู้คืน (RTO) ให้ชัดเจน ดำเนินการทดสอบและทบทวนแผนความต่อเนื่องทางธุรกิจ เป็นประจำ เพื่อให้มั่นใจในความสามารถในการกู้คืนธุรกิจได้ทันเวลาที่ มีบริการขัดข้อง Tencent Cloud ได้ออกแบบและนำกรอบการจัดการความต่อเนื่องของธุรกิจ ที่เหมาะสมกับสภาพแวดล้อมคอมพิวเตอร์คลาวด์ของ ตนเองไปใช้ สร้างระบบการจัดการความต่อเนื่องของธุรกิจที่ครอบคลุม และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจแล้ว เพื่อให้มั่นใจในความพร้อมใช้งานอย่างต่อเนื่องของ ธุรกิจลูกค้า Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภัณฑ์ และบริการคลาวด์ กำหนด RTO และ RPO ของแต่ละธุรกิจให้ชัดเจน และจัดทำกลยุทธ์การตอบสนองและแผนความต่อเนื่องของ ธุรกิจที่แตกต่างกันตามผลการวิเคราะห์ผลกระทบทางธุรกิจ รวมถึงจัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดย ละเอียดสำหรับผลิตภัณฑ์คลาวด์ กลยุทธ์ แผนการ และแผนฉุกเฉินที่เกี่ยวข้องครอบคลุมทุกด้าน เช่น สถานที่ บุคลากร อุปกรณ์ ระบบ ข้อมูล/สารสนเทศ และลำดับความสำคัญของธุรกิจ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะทำการทดสอบฝึกซ้อมความต่อเนื่องของธุรกิจสำหรับผลิตภัณฑ์คลาวด์เป็นประจำตามแผนความต่อเนื่องของธุรกิจ เพื่อให้แน่ใจในความสามารถในการปฏิบัติตามได้จริงของแผนแผนฉุกเฉิน ฯลฯ Tencent Cloud จะประเมินความสมบูรณ์ ความสมเหตุสมผล และประสิทธิภาพของระบบการจัดการความต่อเนื่องของธุรกิจเป็นประจำทุกปี และจะปรับปรุงระบบการจัดการความต่อเนื่องของธุรกิจตามผลการประเมิน Tencent Cloud ยังทบทวนแผนความต่อเนื่องทางธุรกิจทุกปี และอัปเดตแผนตามความจำเป็นตามผลการทบทวน เมื่อมีการเปลี่ยนแปลงครั้งสำคัญในฟังก์ชันทางธุรกิจหรือทรัพยากรที่สำคัญ Tencent Cloud จะทบทวนขอบเขตของธุรกิจและฟังก์ชันสำคัญ และการพึ่งพาองค์ประกอบต่างๆ ของธุรกิจและฟังก์ชันเหล่านั้น และจะแก้ไขแผนความต่อเนื่องทางธุรกิจอย่างทันท่วงที
3.6	การบำรุงรักษาอุปกรณ์ระบบสารสนเทศ	ผู้ให้บริการหรือผู้ประกอบการต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่อง และอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน	ลูกค้าควรทำการบำรุงรักษาอุปกรณ์ระบบเทคโนโลยีสารสนเทศเป็นประจำ เพื่อให้มั่นใจว่าอุปกรณ์ยังคงทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่ดี เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดมาตรฐานการจัดการสินทรัพย์ข้อมูลและกระบวนการจัดการตลอดวงจรชีวิตสินทรัพย์ เพื่อจัดการและปกป้องสินทรัพย์ เช่น ข้อมูลอิเล็กทรอนิกส์ ฮาร์ดแวร์และอุปกรณ์เสมือน โครงสร้างพื้นฐาน ระบบแอปพลิเคชัน และซอฟต์แวร์ โดยจำแนกประเภทและระดับ Tencent Cloud ใช้ระบบการจัดการสินทรัพย์ในการบริหารจัดการอุปกรณ์ฮาร์ดแวร์และส่วนประกอบซอฟต์แวร์ รวมถึงการลงทะเบียนและผูกมัดสินทรัพย์ การตรวจนับและการอัปเดตข้อมูลสินทรัพย์ การปลดระวางและเปลี่ยนใหม่สินทรัพย์ เป็นต้น เพื่อรับประกันการทำงานที่ราบรื่นของระบบพื้นฐานของแพลตฟอร์มคลาวด์ และจัดเตรียมการสนับสนุนที่เชื่อถือได้ให้กับระบบธุรกิจ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			รักษาบัญชีรายละเอียดของฮาร์ดแวร์และสิ่งอำนวยความสะดวก สะดวกในฐานะข้อมูลการจัดการการกำหนดค่า (Configuration Management Database: CMDB) ซึ่งรวมถึงวันที่สิ้นสุดการสนับสนุน (End-of-Support Date) และข้อมูลเวอร์ชันของแพลตฟอร์มสำหรับแต่ละเซิร์ฟเวอร์ Tencent Cloud ดำเนินการปลดระวางและเปลี่ยนเซิร์ฟเวอร์เป็นประจำ ส่วนประกอบประเภทซอฟต์แวร์ (เช่น ระบบปฏิบัติการและระบบฐานข้อมูล) จะถูกเปลี่ยนเป็นเวอร์ชันที่เหมาะสมก่อนวันที่สิ้นสุดการส ับสนุน สำหรับฮาร์ดแวร์ที่ปลดระวางแล้ว Tencent Cloud ใช้วิธีการทำลายทางกายภาพที่ปลอดภัย เพื่อรับประกันว่าฮาร์ดแวร์ถูกทำลายอย่างสมบูรณ์ และมีการบันทึกการไถ่ถอนการทำลาย นอกจากนี้ เจ้าหน้าที่รักษาความปลอดภัยของศูนย์ข้อมูลแต่ละแห่งของ Tencent Cloud จะดำเนินการตรวจสอบสถานการณ์ของห้องเซิร์ฟเวอร์และ อุปกรณ์ต่างๆ อย่างเคร่งครัดตามรายการตรวจสอบและแผนการตรวจสอบ เป็นประจำ และจะลงนามและบันทึกเวลาตรวจสอบที่จุดตรวจแต่ละแห่ง เมื่อพบความขัดข้องของโครงสร้างพื้นฐานหรือเหตุการณ์ ด้านความปลอดภัย จะเริ่มต้นขั้นตอนการตอบสนองเหตุการณ์ของศูนย์ข้อมูล ทันที

10.2.4 การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
4	การตรวจสอบ ความมั่นคงป ลอดภัยทางระ บบสารสนเทศ	ผู้ให้บริการหรือผู้ประกอบการธุรกิจจะต้ องจัดให้มีการตรวจสอบความมั่นคง ปลอดภัย ทางระบบสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่านโยบายและมาตรก าร การรักษาความมั่นคงปลอดภัยทาง ระบบสารสนเทศที่เกี่ยวข้องกับการให้	ลูกค้าควรดำเนินการตรวจสอบความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง เพื่อประเมินประสิทธิภาพและความปลอดภัยของนโยบายและมาตรการความปลอดภัยระบบเทคโนโลยีสารสนเทศ และส่งสำเนาผลการตรวจสอบต่อธนาคารแห่งประเทศไทย ภายใน 45 วันหลังจากเสร็จสิ้นการตรวจสอบ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		บริการเป็นไปอย่างมีประสิทธิภาพ มั่นคงปลอดภัยสามารถให้บริการได้ อย่างต่อเนื่อง พร้อมจัดส่งสำเนาผลการตรวจสอบ ให้ ธปท. ภายใน 45 วันนับแต่วันที่ทำการตรวจสอบแล้ว เสร็จ	จริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเท ศไทย ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยก ายในอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบกา รจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละ หนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และร บบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็น อิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มี ลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการ ล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่ สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจา ก "Compliance Document Download"
5	การทบทวนห รือปรับปรุงมา ตรการการรักร ษาความมั่นคง ปลอดภัยทา งระบบสารสนเทศ	ผู้ให้บริการหรือผู้ประกอบการต้อง ดำเนินการทบทวนหรือปรับปรุงมา ตรการการรักษา ความมั่นคงปลอดภัยทางระบบสารส นเทศอย่างน้อยปีละครั้งหรือเมื่อมีกา รเปลี่ยนแปลงที่ส่งผลกระทบ กับนโยบายและมาตรการที่ได้กำหนด ไว้	ลูกค้าควรดำเนินการปรับปรุงและทบทวนมาตรการความ ปลอดภัยของระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละห ึ่งครั้ง และจัดฝึกอบรมและให้การศึกษาแก่พนักงานที่เกี่ยวข้อง Tencent Cloud จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัย บนคลาวด์สอดคล้องกับนโยบายความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
	ตลอดจนจัดอบรมและให้ความรู้แก่บุคลากรที่เกี่ยวข้อง	นอกจากนี้ผู้ให้บริการหรือผู้ประกอบการ ควรจัดให้มีการพร้อมในการรักษา ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเพื่อรับมือกับภัยคุกคามทางไซเบอร์โดยให้ครอบคลุมถึงการ	มาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบายความปลอดภัยข้อมูล Tencent Cloud ยังได้สร้างกลไกการฝึกอบรมความปลอดภัยข้อมูลที่สมบูรณ์ภายในองค์กร โดยกำหนดให้พนักงานประจำ ที่ปรึกษานักฝึกงาน และพนักงานภายนอก ต้องเรียนหลักสูตรฝึกอบรมความปลอดภัยข้อมูล หลักสูตรฝึกอบรมที่เกี่ยวข้องประกอบด้วยการฝึกอบรมบังคับสำหรับพนักงานทุกคน การฝึกอบรมเฉพาะทางสำหรับตำแหน่งงานสำคัญ และการฝึกอบรมวิชาชีพเลือกได้เอง เป็นต้น โดยเนื้อหาครอบคลุมด้านต่าง ๆ เช่น ความตระหนักรู้ด้านความปลอดภัยพื้นฐาน ความปลอดภัยในการทำงาน การระบุและป้องกันช่องโหว่ การปกป้องความเป็นส่วนตัว การตอบสนองเหตุการณ์ มาตรฐานความปลอดภัยในการพัฒนา และข้อกำหนดด้านความปลอดภัยของข้อมูล

11

Tencent Cloud จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ SEC เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี ระบบเทคโนโลยีสารสนเทศ อย่างไร

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (SEC) ได้ออก [SEC No. Sor Thor 38/2565](#) เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี ระบบเทคโนโลยีสารสนเทศ ในเดือนกันยายน 2565

ซึ่งกำหนดให้ผู้ประกอบธุรกิจบริการหลักทรัพย์ดำเนินการประเมินระดับความเสี่ยงเป็นประจำ เพื่อประเมินระดับผลกระทบของระบบเทคโนโลยีสารสนเทศที่มีต่อการดำเนินงานทางธุรกิจ ในปี 2567 SEC ได้ออก [SEC No. Nor Thor 33/2567](#) เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี ระบบเทคโนโลยีสารสนเทศ เพิ่มเติม ซึ่งเป็นการแก้ไขและปรับปรุงระเบียบก่อนหน้า

ยกระดับข้อกำหนดทางกฎระเบียบโดยสมบูรณ์ โดยมีวัตถุประสงค์เพื่อเสริมสร้างมาตรฐานการปฏิบัติตามข้อกำหนดของหน่วยงานในตลาดทุนไทย (รวมถึงบริษัทหลักทรัพย์ บริษัทจัดการกองทุน ตลาดหลักทรัพย์ ฯลฯ) ด้านการพัฒนา การดำเนินงาน ความปลอดภัย และการจัดการความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

ระเบียบดังกล่าวจัดเตรียมแนวทางปฏิบัติที่ดีสำหรับการกำกับดูแลด้านเทคโนโลยีสารสนเทศ การรับประกันความปลอดภัยเทคโนโลยีสารสนเทศ และการดำเนินการตรวจสอบแก่ผู้ประกอบธุรกิจบริการหลักทรัพย์ ผ่านเอกสารสนับสนุน เช่น ภาคผนวก 2 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และ ภาคผนวก 4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ในบทนี้ Tencent Cloud จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จากภาคผนวก 2-4 ของ ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มี ระบบเทคโนโลยีสารสนเทศ และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud จะช่วยผู้ประกอบธุรกิจบริการหลักทรัพย์ในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

11.1 เรื่อง กฎระเบียบอย่างละเอียดในการจัดตั้งระบบเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
4	การประเมินระดับความเสี่ยง	เพื่อประโยชน์ในการปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ ให้ผู้ประกอบธุรกิจประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบธุรกิจ ตามแบบ RLA (Risk Level Assessment) และจัดส่งผลการประเมินดังกล่าวต่อสำนักงาน ภายในไตรมาสที่ 1 ของทุกปี ทั้งนี้ ตามแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงานผลการประเมินระดับความเสี่ยงตามวรรคหนึ่ง ต้องผ่านการพิจารณาจากคณะกรรมการหรือผู้ที่ได้รับมอบหมายจากคณะ	ลูกค้าควรดำเนินการประเมินระดับความเสี่ยงระบบเทคโนโลยีสารสนเทศเป็นประจำทุกปี และส่งผลการประเมินตามรูปแบบและวิธีการที่สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์กำหนด ภายในไตรมาสแรกของทุกปี Tencent Cloud จะให้ความร่วมมือตามสถานการณ์จริงและตามข้อตกลงที่ตกลงกับลูกค้า ในการตรวจสอบความปลอดภัยและการกำกับดูแลของบุคคลที่สามของลูกค้า และจัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบที่ลูกค้าเป็นผู้ริเริ่มอย่างแข็งขัน Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		กรรมการของผู้ประกอบธุรกิจให้รับผิดชอบในเรื่องดังกล่าว	ยังได้รับการตรวจสอบโดยบุคคลที่สามอิสระมืออาชีพเป็นประจำ โดยผ่านการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง

11.2 ภาคผนวก 2 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
2.2	นโยบายความ เสี่ยงด้านเทคโนโลยีสารสนเทศ	2.2 ผู้ประกอบธุรกิจต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมาย	ลูกค้าควรกำหนดและบำรุงรักษานโยบายและขั้นตอนที่เกี่ยวข้องกับการกำกับดูแลและการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดำเนินการทบทวนและอัปเดตเป็นประจำ และควรสื่อสารนโยบายดังกล่าวไปยังบุคคลที่เกี่ยวข้องเพื่อการเรียนรู้และการปฏิบัติตาม
		2.2.1 นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy)	เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูลซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยข้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย
		2.2.2 นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy)	เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดการความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ รวมถึงขึ้นการทำงานประจำวันและกระบวนการจัดการของหน่วยงานและพนักงานทุกหน่วยในบริษัท
2.3	การสื่อสารนโยบายไปยังบุคคลที่เกี่ยวข้อง	2.3 ผู้ประกอบธุรกิจต้องจัดให้มีการดำเนินการตามนโยบายในข้อ 2.2 ดังนี้	นโยบายความปลอดภัยข้อมูลของ Tencent Cloud จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัยบนคลาวด์สอดคล้องกับนโยบายความปลอดภัย มาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง
		2.3.1 สื่อสารนโยบายตามข้อ 2.2 ให้แก่บุคคลที่เกี่ยวข้อง รับทราบตามบทบาทหน้าที่ความรับผิดชอบ และสิทธิการเข้าถึงข้อมูล ในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคคลที่เกี่ยวข้องดังกล่าวเข้า	และรับประกันความเพียงพอและประสิทธิผลของนโยบายความปลอดภัยข้อมูล นอกจากนี้ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
2.4	การทบทวนแ ละอัปเดตนโยบาย	ใจและสามารถปฏิบัติ ตามนโยบายได้อย่างถูกต้อง 2.3.2 กำหนดขั้นตอนและวิธีปฏิบัติ งานให้เป็นไปตามนโยบายตามข้อ 2.2 2.3.3 ในกรณีที่มีการเปลี่ยนแปลงนโ บายตามข้อ 2.2 ต้องสื่อสารให้บุคคล ที่เกี่ยวข้องได้รับทราบ อย่างทั่วถึง และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติ งานให้สอดคล้องกับการเปลี่ยนแปลง ดังกล่าว	ได้สร้างกรอบการจัดการความเสี่ยงที่ครอบคลุมตามมาตรฐาน ISO/IEC 27001:2022 และดำเนินกิจกรรมการประเมินความเสี่ยงด้านความปลอดภัยข้อมูลอย่างน้อยปีละหนึ่งครั้ง พนักงานสามารถดูนโยบายเหล่านี้ที่ Tencent Cloud เผยแพร่ผ่านแพลตฟอร์มภายในได้ Tencent Cloud ได้สร้างกลไกการฝึกอบรมความปลอดภัยข้อมูลที่เหมาะสมภายในองค์กร จัดเตรียมหลักสูตรฝึกอบรมที่หลากหลาย รวมถึงการฝึกอบรมบังคับสำหรับพนักงานทุกคน การฝึกอบรมเฉพาะทางสำหรับตำแหน่งงานสำคัญ และการฝึกอบรมวิชาชีพเลือกได้เอง เป็นต้น โดยเนื้อหาครอบคลุมด้านต่างๆ เช่น ความตระหนักรู้ด้านความปลอดภัยพื้นฐาน ความปลอดภัยในการทำงาน การระบุและป้องกันช่องโหว่ การปกป้องความเป็นส่วนตัว การตอบสนองเหตุการณ์ มาตรฐานความปลอดภัยในการพัฒนา และข้อกำหนดด้านความปลอดภัยของข้อมูล Tencent Cloud
		2.4 ผู้ประกอบธุรกิจต้องทบทวนหรือ ปรับปรุงนโยบายตามข้อ 2.2 อย่างน้อยปีละ 1 ครั้ง และ โดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อภารกิจกับดูแล และบริหารจัดการความเสี่ยงด้าน IT อย่างมีนัยสำคัญ	มุ่งมั่นที่จะผนวกรวมการจัดการความปลอดภัยข้อมูลเข้ากับงานจัดการในชีวิตประจำวัน เพื่อให้มั่นใจว่าพนักงานเข้าใจและปฏิบัติตามนโยบายและข้อกำหนดการจัดการความปลอดภัยข้อมูลภายใน นอกจากนี้ Tencent Cloud ยังได้รับใบรับรองและคุณวุฒิด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดความเป็นส่วนตัวหลายรายการ เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, SOC ซึ่งพิสูจน์ว่าการจัดการความปลอดภัยและการสร้างการป้องกันข้อมูลส่วนบุคคลของ Tencent Cloud เป็นไปตามมาตรฐานการรับรองที่เกี่ยวข้องหรือแนวปฏิบัติที่ดีของอุตสาหกรรม และยังได้รับการตรวจสอบจากสถาบันตรวจสอบบุคคลที่สามมืออาชีพเป็นประจำอีกด้วย

11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
1	โครงสร้างการ บริหารงานเพื่ การรักษาคว ามมั่นคงปลอ ดภัยด้าน IT	ผู้ประกอบการต้องดำเนินการจัดให้มี โครงสร้างดังกล่าว โดยมีลักษณะอย่างน้อยดังนี้ 1.1 กำหนดโครงสร้างภายในองค์กร (organizational structure) ในการปฏิบัติงานด้าน IT โดยมี รายละเอียดหน้าที่และความรับผิดชอบ ของบุคลากรเป็นลายลักษณ์อักษร 1.2 มีการสอบทานการปฏิบัติงานเพื่อ ป้องกันความเสี่ยงในการรักษาความม ั่นคงปลอดภัยของระบบ IT ที่อาจเกิดขึ้นในการปฏิบัติงาน	ลูกค้าควรสร้างโครงสร้างองค์กรด้านความปลอดภัยเทคโนโลยีสารสนเทศ กำหนดบทบาทและความรับผิดชอบให้ชัดเจน โดยใช้การแบ่งแยกหน้าที่และการทบทวนการดำเนินงานเป็นประจำ เพื่อป้องกันความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศในระหว่างกระบวนการดำเนินงาน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านโครงสร้างองค์กรด้านการจัดการความปลอดภัยเทคโนโลยีสารสนเทศ Tencent Cloud ได้สร้างโครงสร้างองค์กรที่เกี่ยวข้องกับความปลอดภัยบนคลาวด์และความปลอดภัยข้อมูล กำหนดบทบาทหน้าที่ด้านความปลอดภัยและความรับผิดชอบที่เกี่ยวข้องในระดับต่างๆ ให้ชัดเจน และกำหนดกลไกการทำงานสำหรับการตรวจสอบความปลอดภัยข้อมูลและการประเมินความเสี่ยงด้านความปลอดภัยข้อมูล Tencent Cloud ได้จัดตั้งคณะกรรมการเทคโนโลยีความปลอดภัยและทีมงานความปลอดภัยมืออาชีพที่มีหน้าที่และสาขาวิชาที่แตกต่างกัน Tencent Cloud รวบรวมทีมบริการผู้เชี่ยวชาญที่มีประสบการณ์ในอุตสาหกรรม มุ่งมั่นให้บริการผลิตภัณฑ์และบริการที่ปลอดภัย น่าเชื่อถือ เป็นมืออาชีพ และเป็นไปตามข้อกำหนดของลูกค้า Tencent Cloud ยังกำหนดองค์ประกอบของเจ้าหน้าที่ประสานงานด้านความปลอดภัยข้อมูล (Information Security Liaison Officer) โดยเจ้าหน้าที่ประสานงานด้านความปลอดภัยข้อมูลในแต่ละภูมิภาคจะรักษาการสื่อสารที่ราบรื่นกับหน่วยงานกำกับดูแลท้องถิ่นและลูกค้าตามข้อกำหนดการปฏิบัติตามและความต้องการทางธุรกิจ เพื่อให้มั่นใจว่า Tencent Cloud ปฏิบัติตามกฎหมาย กฎระเบียบ และข้อตกลงตามสัญญา ในด้านการทบทวนการดำเนินงาน Tencent Cloud ยังได้กำหนดกลยุทธ์การให้สิทธิ์และกลไกเมทริกซ์การแบ่งแยกสิทธิ์ภายในองค์กร และรักษาบันทึกข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Tencent Cloud จัดงานตรวจสอบสิทธิ์ภายในเป็นประจำเพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์สำหรับสิทธิ์การเข้าถึงที่ไม่จำเป็นอีกต่อไป จะดำเนินการมาตรการที่เหมาะสมและเพิกถอนสิทธิ์การเข้าถึงที่ไม่จำเป็นทันที Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยสถานะการเข้าสู่ระบบบัญชีพนักงานแบบเรียลไทม์ ทันทีที่ตรวจพบพฤติกรรมหรือการเข้าสู่ระบบที่ผิดปกติใดๆ ระบบจะติดต่อเจ้าของบัญชีทันทีเพื่อดำเนินการตรวจสอบและจัดการ และบันทึกเหตุการณ์ที่เกี่ยวข้องอย่างละเอียด สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้ เครื่องบินคุ้มกัน อย่างเต็มรูปแบบ โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบแบ็กเอนด์จากส่วนกลางผ่าน เครื่องบินคุ้มกัน การเข้าถึง เครื่องบินคุ้มกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติสิทธิ์ มีเฉพาะเจ้าหน้าที่ปฏิบัติการภายในของ Tencent Cloud บางส่วนเท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบ เครื่องบินคุ้มกัน ต้องการการยืนยันตัวตนสองปัจจัย บันทึกการดำเนินการปฏิบัติการจะถูกเก็บไว้โดยศูนย์กลางแพลตฟอร์มบันทึก (log) และได้รับการตรวจสอบโดยทีมตรวจสอบภายในของ Tencent Cloud เป็นประจำ
2.1	บุคลากรที่เกี่ยวข้องหรือที่ให้บริการระบบ IT ปฏิบัติงาน	ผู้ประกอบการต้องบริหารจัดการบุคลากรตามข้อ 2.1 อย่างเหมาะสม โดยดำเนินการอย่างน้อยดังนี้ (1) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ดังนี้ (1.1) คำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน (1.2) การตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอ และสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ (2) มีข้อกำหนดให้บุคลากรทำความเข้าใจ รับทราบ และลงนามยอมรับ	ลูกค้าควรจัดการบุคลากรที่เกี่ยวข้องหรือใช้ระบบเทคโนโลยีสารสนเทศในการดำเนินงานอย่างเหมาะสม เช่น การสร้างกระบวนการคัดเลือกบุคลากร การลงนามในข้อตกลงรักษาความลับกับพนักงาน การดำเนินกิจกรรมสร้างจิตสำนึกเกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ การกำหนดมาตรการลงโทษสำหรับการละเมิด และกลไกการจัดการเมื่อพนักงานลาออกหรือเปลี่ยนตำแหน่ง เป็นต้น เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานและขั้นตอนการจัดการทรัพยากรบุคคลที่สมบูรณ์ เพื่อให้มั่นใจในการคัดเลือก จ้าง และจัดวางบุคลากรตามข้อกำหนดของตำแหน่งงาน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ในเรื่องดังนี้	Tencent Cloud
		(2.1) บทบาทหน้าที่และความรับผิดชอบ ของบุคลากรดังกล่าวเกี่ยวกับ การรักษาความมั่นคงปลอดภัยด้าน IT	ได้สร้างวงจรชีวิตการทำงานที่ชัดเจน ซึ่งรวมถึงขั้นตอนก่อนเข้าทำงาน ขั้นตอนระหว่างการทำงาน และขั้นตอนการลาออก
		(2.2) non-disclosure agreement	ก่อนเข้าทำงาน ผู้สมัครจะต้องผ่านการสัมภาษณ์ โดย Tencent Cloud
		(3) สร้างความตระหนักรู้ถึงความเสี่ยง ด้าน IT ให้แก่บุคลากรซึ่งสามารถ เข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถ ใช้งานระบบ IT ได้อย่างปลอดภัย	จะประเมินว่าตนมีคุณสมบัติตรงตามความสามารถที่ตำแหน่งงานต้องการหรือไม่ ตามกฎหมายที่ใช้บังคับและระดับตำแหน่งงาน ฝ่ายทรัพยากรบุคคลจะทำการตรวจสอบประวัติของผู้สมัครก่อนการจ้างงาน
		(4) กำหนดให้บุคลากรงดเว้นการใช้งาน ระบบ IT ในลักษณะที่อาจก่อให้เกิด ความเสียหายแก่ผู้ประกอบการ ตลาดทุนโดยรวม หรือที่เป็น การกระทำผิดกฎหมาย หรือข้อกำหนดและจรรยาบรรณที่ผู้ประกอบการกำหนดไว้ (ถ้ามี)	การตรวจสอบประวัติรวมถึงประวัติการทำงานในอดีต การตรวจสอบประวัติอาชญากรรม และการตรวจสอบวุฒิการศึกษา ผลการตรวจสอบประวัติจะถูกบันทึกไว้ในระบบการจัดการทรัพยากรบุคคลของ Tencent Cloud
		(5) กำหนดมาตรการในการลงโทษบุคลากร ที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตาม นโยบายและมาตรการรักษาความ มั่นคงปลอดภัยในการปฏิบัติงานด้าน IT	หลังจากรับเข้าทำงาน พนักงานภายในทุกคนต้องลงนามในสัญญาจ้างและข้อตกลงรักษาความลับ โดยสัญญาจ้างได้ระบุกลยุทธ์ความปลอดภัยที่มีอยู่ของ Tencent Cloud
		(6) กำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุด การจ้างงาน หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน เพื่อป้องกันการละเมิดหรือความเสียหาย ที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT	รวมถึงความรับผิดชอบด้านความปลอดภัยข้อมูลและความรับผิดชอบในการปกป้องข้อมูลส่วนบุคคลที่พนักงานหรือบุคคลที่สามต้องปฏิบัติตาม ส่วนข้อตกลงรักษาความลับประกอบด้วยข้อผูกพันและความรับผิดชอบในการรักษาความลับของบุคคลที่ลงนาม และบทลงโทษที่อาจได้รับหากมีการละเมิดข้อกำหนดในการรักษาความลับ พนักงานภายนอก (Outsourcing) ก็จำเป็นต้องได้รับการตรวจสอบประวัติก่อนการจ้างงานเช่นเดียวกัน และต้องปฏิบัติตามข้อกำหนดในการรักษาความลับที่กำหนดไว้ในข้อตกลงระหว่าง Tencent Cloud กับผู้ให้บริการภายนอก ข้อกำหนดในการรักษาความลับระหว่าง Tencent Cloud กับพนักงานและบุคคลที่สามจะได้รับการทบทวนและปรับปรุงโดยฝ่ายกฎหมายตามความจำเป็น ในระหว่างการทำงานของพนักงานหรือบุคคลที่สาม Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ได้สร้างกลไกการฝึกอบรมและการเรียนรู้ด้านความปลอดภัยข้อมูลหลายชุด เพื่อให้ความรู้แก่พนักงานเกี่ยวกับนโยบาย ขั้นตอน และแนวทางปฏิบัติด้านความปลอดภัยข้อมูล พนักงานต้องเข้ารับการฝึกอบรมสร้างจิตสำนึกด้านความปลอดภัยข้อมูลเป็นประจำ ขั้นตอนการลาออกจาก Tencent Cloud รวมถึงการยกเลิกบัญชีผู้ใช้และสิทธิ์การเข้าถึงพื้นที่ ตลอดจนกระบวนการเรียกคืนทรัพย์สินของบริษัท เป็นต้น ทรัพย์สินที่มีตัวตนของ Tencent Cloud ถูกจัดสรรให้กับผู้รับผิดชอบที่กำหนดและถูกบันทึกไว้ผ่านระบบติดตามทรัพย์สินเฉพาะภายในของ Tencent Cloud Tencent Cloud จะทำการตรวจนับทรัพย์สินเป็นประจำเพื่อยืนยันการมีอยู่จริงของทรัพย์สิน และบันทึกผลการตรวจนับ ในด้านการลงโทษทางวินัย Tencent Cloud ได้สร้างขั้นตอนการลงโทษทางวินัยสำหรับพนักงานที่ไม่ปฏิบัติตามข้อกำหนด นโยบาย และขั้นตอนที่กำหนดไว้ การลงโทษทางวินัยที่อาจเกิดขึ้นรวมถึงการไล่ออก การฟ้องร้อง และ/หรือการดำเนินคดีอาญา Tencent Cloud ได้กำหนดประมวลการปฏิบัติสำหรับพนักงาน และเผยแพร่บนแพลตฟอร์มภายใน สำหรับพฤติกรรมที่ละเมิดข้อกำหนดด้านความปลอดภัยและคำวินิจฉัยลงโทษก็จะประกาศในระบบภายในด้วยเช่นกัน
2.2	บุคคลภายนอก ในกรณีที่	ผู้ประกอบการมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้ 2.2.1 ใช้บริการงานด้าน IT จากบุคคลภายนอก 2.2.2 เชื่อมต่อระบบ IT กับบุคคลภายนอก 2.2.3 อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบการหรือข้อมูลของลูกค้าที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของผู้ประกอบการ ผู้ประกอบการต้องบริหารจัดการบุคคลภายนอกตามข้อ 2.2.1 , 2.2.2	ลูกค้าควรจัดการบุคลากรภายนอกที่เกี่ยวข้องหรือใช้ระบบเทคโนโลยีสารสนเทศ เช่น ดำเนินการตรวจสอบอย่างละเอียด (Due Diligence) การลงนามในสัญญาและข้อตกลงรักษาความลับกับบุคลากรภายนอก การประเมินความเสี่ยงและการตรวจสอบเป็นประจำ และการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ เป็นต้น ในด้านการตรวจสอบอย่างละเอียด เมื่อลูกค้าขอ Tencent Cloud จะให้ความร่วมมืออย่างแข็งขันในการจัดเตรียมข้อมูลเพื่อให้ลูกค้าสามารถดำเนินการตรวจสอบอย่างละเอียดให้เสร็จสิ้น เนื้อหาเพิ่มเติมเกี่ยวกับการตรวจสอบอย่างละเอียดสาม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		หรือ 2.2.3 ดังนี้	ารถดูได้ในภาคผนวก 3-2 "
		(1) ประเมินความเสี่ยงจากการใช้บริกา ร การเชื่อมต่อหรือการเข้าถึงข้อมูล จากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก (ถ้ามี)	การคัดเลือกผู้ให้บริการภายนอก ของบทที่ 6 " Tencent Cloud จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก ของ BOT อย่างไร" ได้อย่างไร" ในคู่มือนี้
		(2) กำหนดวิธีปฏิบัติและหลักเกณฑ์ใน การคัดเลือกบุคคลภายนอก	สำหรับการลงนามในสัญญา Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็น ทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement
		(3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบธ กิจและบุคคลภายนอกอย่างชัดเจนแล ะเป็นลายลักษณ์อักษร	ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งส องฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้
		(4) กรณีบุคคลภายนอกซึ่งเป็นผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญตาม ผลการประเมินความเสี่ยงในข้อ 2.2 (1) ข้อตกลงหรือสัญญาการให้บริการ ต้องระบุสิทธิให้ผู้ประกอบธุรกิจ สำนักงาน และผู้ตรวจสอบภายนอกที่ได้รับ การแต่งตั้งจากผู้ประกอบธุรกิจหรือสำ นักงาน สามารถเข้าตรวจสอบ การดำเนินงานและการควบคุมภายใน ของบุคคลภายนอกดังกล่าวได้	สำหรับการตรวจสอบและการประเมิน เพื่อสนับสนุนข้อกำหนดการตรวจสอบบุคคลที่สามขอ งลูกค้า Tencent Cloud จะให้ความร่วมมือตามสถานการณ์จริงและตามข้อตกลง ที่ตกลงกับลูกค้า ในการตรวจสอบความปลอดภัยและการกำกับดูแลของ บุคคลที่สามของลูกค้า และจัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและ สนับสนุนกิจกรรมการตรวจสอบที่ลูกค้าเป็นผู้ริเริ่มอย่าง แข็งขัน
		(5) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับ ดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึง ข้อมูลสำคัญของผู้ประกอบธุรกิจหรือ ข้อมูลของลูกค้า	Tencent Cloud โดยลูกค้า ในเวลาเดียวกัน ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปี ละหนึ่งครั้ง และตรวจสอบสถานการณ์ของแพลตฟอร์มคลาวด์และ ระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตาม กฎหมาย ระเบียบข้อบังคับ และมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง
		(6) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใ ้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจาก บุคคลภายนอก โดยต้องสอดคล้องกับ ระดับความเสี่ยงและระดับความมีนัยสำ คัญของบุคคลภายนอก	Tencent Cloud
		(7) รักษาความมั่นคงปลอดภัยด้าน IT	

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		จากการใช้บริการ การเชื่อมต่อหรือ การเข้าถึงข้อมูลจากบุคคลภายนอก ที่สอดคล้องกับการรักษาความมั่นคง ปลอดภัยด้าน IT ของผู้ประกอบการธุรกิจ หรือสอดคล้องกับมาตรฐานสากล ที่ได้รับการยอมรับโดยทั่วไป (8)เตรียมความพร้อมรับมือต่อเหตุกา รณภัยด้าน IT ที่อาจเกิดขึ้น และมีผลกระทบอย่างมีนัยสำคัญ เพื่อให้สามารถให้บริการหรือดำเนินธุ รกิจ ได้อย่างต่อเนื่อง	ยังได้รับการตรวจสอบโดยบุคคลที่สามอิสระมืออาชีพเป นประจำ โดยผ่านการจัดทำรายงานการควบคุมระบบและองค์กร ที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริกา รล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง ในด้านการตอบสนองต่อเหตุการณ์ผิดปกติด้าน เทคโนโลยีสารสนเทศ Tencent Cloud คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการในงาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับ ระบบในงานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับในงานของลูกค้าผ่านกลไ กการตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมแล ะจัดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้า ได้รับการตอบสนองและจัดการอย่างทันท่วงที นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเ เป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พ บบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้า ได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเว ลา ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับกา รสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
3	การบริหารจัดการทรัพยากรสิน ด้าน IT	ผู้ประกอบการต้องจัดให้มีการบริหาร จัดการทรัพยากรสินด้าน IT เพื่อนำไปใช้ดำเนินการเกี่ยวกับการรั กษา ความมั่นคงปลอดภัยด้าน IT ได้อย่างเหมาะสม ครบถ้วนและเป็นปัจจุบัน ดังนี้	ลูกค้าควรบำรุงรักษาบัญชีรายการสินทรัพย์ที่ประกอบ ด้วยสินทรัพย์ข้อมูลทั้งหมด และสร้างกลไกการจัดการสินทรัพย์ข้อมูลเพื่อระบุสินทรัพย์ จัดระดับและหมวดหมู่ กำหนดกรรมสิทธิ์ในสินทรัพย์ และจัดการความปลอดภัยของสินทรัพย์ตามระดับที่แตก ต่างกัน บัญชีรายการสินทรัพย์ควรได้รับการทบทวนเป็นประจำ และควรได้รับการปรับปรุงให้ทันสมัยทันทีเมื่อมีการเปลี่ย นแปลง
		3.1 จัดทำทะเบียนรายการทรัพยากรสินด้าน IT ประเภทฮาร์ดแวร์ ซอฟต์แวร์รวมถึงสิทธิ์ในการใช้งาน ฮาร์ดแวร์และซอฟต์แวร์	เพื่อช่วยเหลือลูกค้าในการบริหารสินทรัพย์ข้อมูลอย่าง ครอบคลุม Tencent Cloud Cloud Workload Protection Platform (CWPP) ซึ่งสนับสนุนการรวบรวมลายเซ็นดิจิทัลของสินทรัพย์โ ดยอัตโนมัติ และบริหารจัดการข้อมูลลายเซ็นดิจิทัลของสินทรัพย์ เช่น บัญชีผู้ใช้ พอร์ต กระบวนการ และแอปพลิเคชัน อย่างเป็นเอกภาพ CWPP ยังสามารถดำเนินการตรวจสอบอย่างรวดเร็วเกี่ยวกับขอ อบเขตผลกระทบความเสี่ยงของเหตุการณ์ความปลอดภัย ที่เกิดขึ้นแล้ว ตามลายเซ็นดิจิทัลของสินทรัพย์ เพื่อช่วยลูกค้ายกระดับความปลอดภัยของเซิร์ฟเวอร์ ลูกค้ายังสามารถใช้แพลตฟอร์มการจัดการความปลอดภัย แบบครบวงจร Cloud Security Center (CSC) ของ Tencent Cloud
		3.2 กำหนดบุคคลหรือหน่วยงานซึ่งรับ ผิดชอบทรัพยากรสินด้าน IT แต่ละรายการ	เพื่อบริหารจัดการความปลอดภัยของสินทรัพย์ข้อมูล CSC มีฟังก์ชันศูนย์ความปลอดภัยสินทรัพย์ ซึ่งช่วยให้ลูกค้าสามารถตรวจนับสินทรัพย์บนคลาวด์แ บบไดนามิกโดยอัตโนมัติ รวมถึงเซิร์ฟเวอร์คลาวด์ ที่เก็บวัตถุ ฐานข้อมูลคลาวด์ โหลดบาลานเซอร์ เป็นต้น และบริหารจัดการความเสี่ยงด้านความปลอดภัยของสิ นทรัพย์แบบครบวงจรผ่านหลายมิติความปลอดภัย เช่น ความเสี่ยงการกำหนดค่าคลาวด์ ช่องโหว่ และเหตุการณ์ความปลอดภัย เพื่อลดความเสี่ยง "IT ล่องหน" บนคลาวด์
		3.3 จัดให้มีการบำรุงรักษาทรัพยากรสินด้าน IT อย่างสม่ำเสมอ	เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำ กับดูแล Tencent Cloud ได้กำหนดมาตรฐานการจัดการสินทรัพย์ข้อมูลและกระ บวนการจัดการตลอดวงจรชีวิตสินทรัพย์ เพื่อจัดการและปกป้องสินทรัพย์ เช่น

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
4	การรักษาความมั่นคงปลอดภัยของข้อมูล	ผู้ประกอบธุรกิจต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อให้ข้อมูลมีความถูกต้องครบถ้วนและมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม ดังนี้ 4.1การกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล 4.2การจัดชั้นความลับของข้อมูล (data classification) และแนวทางการรักษาความปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับ 4.3การจัดให้มีแนวทางในการนำเข้าประมวลผล และทำลายข้อมูลอย่างปลอดภัย 4.4การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data Inventory) ให้ครบถ้วนและเป็นปัจจุบัน	ข้อมูลอิเล็กทรอนิกส์ ฮาร์ดแวร์และอุปกรณ์เสมือน โครงสร้างพื้นฐาน ระบบแอปพลิเคชัน และซอฟต์แวร์ โดยจำแนกประเภทและระดับ Tencent Cloud ใช้ระบบการจัดการสินทรัพย์ในการบริหารจัดการอุปกรณ์ฮาร์ดแวร์และส่วนประกอบซอฟต์แวร์ รวมถึงการลงทะเบียนและผูกมัดสินทรัพย์ การตรวจสอบและการอัปเดตข้อมูลสินทรัพย์ การปลดระวางและเปลี่ยนใหม่สินทรัพย์ เป็นต้น เพื่อรับประกันการทำงานที่ราบรื่นของระบบพื้นฐานของแพลตฟอร์มคลาวด์ และจัดเตรียมการสนับสนุนที่เชื่อถือได้ให้กับระบบธุรกิจ ลูกค้าควรกำหนดกลไกการปกป้องความปลอดภัยของข้อมูล โดยจำแนกประเภทข้อมูลตามระดับความอ่อนไหวและความสำคัญ และดำเนินการป้องกันการป้องกันข้อมูลตามระดับข้อมูลที่แตกต่างกัน นอกจากนี้ ลูกค้าควรกำหนดขั้นตอนการทำลายข้อมูลให้ชัดเจน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการจำแนกประเภทและระดับข้อมูล Data Security Governance Center (DSGC) สามารถช่วยลูกค้าจัดการสินทรัพย์ข้อมูลโดยอัตโนมัติ จัดประเภทและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลขององค์กรบนคลาวด์ โดยได้รับอนุญาตจากองค์กร DSGC จะเชื่อมต่อกับสินทรัพย์ข้อมูลประเภทต่างๆ บนคลาวด์อย่างลึกซึ้ง และรับข้อมูลสินทรัพย์ข้อมูลที่ทันเวลาจากมิติภายในตามลักษณะของข้อมูล DSGC จะช่วยองค์กรค้นพบข้อมูลที่ละเอียดอ่อนอย่างเจาะจง และจัดระเบียบสินทรัพย์ข้อมูลจากมุมมองความปลอดภัย ตามมาตรฐานการจำแนกประเภทและระดับข้อมูลระดับชาติ อุตสาหกรรม หรือองค์กร DSGC จะช่วยองค์กรในการจำแนกประเภทและระดับข้อมูล Tencent Cloud ได้สร้างมาตรฐานการจำแนกประเภทและระดับข้อมูลที่สมบูรณ์ภายในองค์กร โดยข้อมูลทั้งหมดจะถูกจำแนกประเภทและระดับตามมาตรฐานนี้เป็นเอกภาพตั้งแต่เริ่มสร้าง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ข้อมูลของลูกค้าภายใน Tencent Cloud จัดอยู่ในระดับความปลอดภัยสูง สำหรับพนักงานภายใน Tencent Cloud หากไม่ใช้บริการที่ลูกค้าเลือกใช้ซึ่งจำเป็นต้องประมวลผลข้อมูลของลูกค้า พนักงาน Tencent Cloud จะไม่พยายามเข้าถึงข้อมูลลูกค้าใดๆ ในด้านการป้องกันการจัดเก็บข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสานรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล Key Management Service (KMS) ใช้โมดูลความปลอดภัยฮาร์ดแวร์ (HSM) ที่ได้รับการรับรอง FIPS-140-2 ในการสร้างและปกป้องคีย์ และสามารถสนับสนุนการจัดการวงจรชีวิตเต็มรูปแบบของคีย์การเข้ารหัสของลูกค้า ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้นั้นก็มีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า นอกจากนี้ ลูกค้ายังสามารถใช้บริการ Tencent Cloud ต่อไปเพื่อให้บรรลุการถ่ายโอนข้อมูลที่ปลอดภัยในสถานการณ์ต่างๆ: Direct Connect (DC): จัดเตรียมการเชื่อมต่อเครือข่ายแบนด์วิดท์สูงที่มีความเฉพาะตัวและความปลอดภัยสูง ผู้ใช้เป็นเจ้าของลิงก์เครือข่ายโดยเฉพาะ ไม่มีความเสี่ยงข้อมูลรั่วไหล VPN Connection:

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		5.3 กำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชีprivileged user (privileged user management)	Tencent Cloud ยังได้กำหนดกลยุทธ์การอนุมัติสำหรับการควบคุมการเข้าถึงและกลไกเมทริกซ์การแยกอำนาจภายในองค์กร โดยกำหนดให้บัญชีผู้ใช้ต้องใช้ตัวระบุเฉพาะ และตั้งค่านโยบายรหัสผ่านสำหรับบัญชีพนักงานตามแนวทางความปลอดภัยขั้นพื้นฐาน ซึ่งรวมถึงความยาวรหัสผ่าน ความซับซ้อน การล๊อค และการรีเซต เป็นต้น สำหรับอุปกรณ์ปลายทาง ระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายภายใน Tencent Cloud ได้กำหนดค่าการจำกัดจำนวนครั้งในการเข้าสู่ระบบที่ล้มเหลวและนโยบายหมดเวลาการทำงานของเซสชัน Tencent Cloud ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการตรวจสอบสิทธิ์การเข้าถึงของพนักงาน โดยผู้ใช้ต้องผ่านการยืนยันตัวตนสองปัจจัยก่อนเข้าถึงทรัพยากรภายใน Tencent Cloud ปฏิบัติตามหลักการสิทธิ์น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิ์น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิ์เฉพาะก็ต่อเมื่อมีความจำเป็นต้องใช้ และผ่านกระบวนการอนุมัติสิทธิ์ที่เข้มงวดเท่านั้น Tencent Cloud จะรักษาบันทึกข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดงานตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยสถานะการเข้าสู่ระบบบัญชีพนักงานแบบเรียลไทม์ ทันทีที่ตรวจพบพฤติกรรมการณ์การเข้าสู่ระบบที่ผิดปกติใดๆ ระบบจะติดต่อเจ้าของบัญชีทันทีเพื่อดำเนินการตรวจสอบและจัดการ และบันทึกเหตุการณ์ที่เกี่ยวข้องอย่างละเอียด สำหรับผู้ที่มีสิทธิ์สูง ลูกค้าสามารถใช้ Cloud Access Management (CAM) เพื่อมอบสิทธิ์การเข้าถึงทรัพยากรให้กับผู้ใช้ย่อยผ่านวิธีการต่างๆ เช่น แท็ก เพื่อให้บรรลุการควบคุมการเข้าถึงทรัพยากรคลาวด์อย่างละเอียด CAM ยังสนับสนุนการดูและติดตามบันทึกการดำเนินการของพนักงานผ่าน CloudAudit นอกจากนี้ Tencent

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Cloud ยังให้บริการ Bastion Host (BH) ที่สามารถสนับสนุนการอนุญาตอย่างละเอียดตามมิติต่างๆ เช่น ผู้ใช้ สิทธิ์ทรัพยากร บัญชีผู้ใช้ และสิทธิ์การดำเนินการ เพื่อให้มั่นใจว่าสิทธิ์ที่ผู้ใช้มีอยู่เป็นสิทธิ์ขั้นต่ำที่จำเป็นสำหรับการเข้าถึงสิทธิ์และทำงานให้สำเร็จ เครื่องบินคุ้มกัน ยังสนับสนุนฟังก์ชันการตรวจสอบการดำเนินการ โดยบันทึกและวิเคราะห์บันทึกการดำเนินการของผู้ใช้ เพื่อให้มั่นใจว่าสามารถติดตามเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพ ภายใน Tencent Cloud ยังได้กำหนดข้อกำหนดการจัดการสำหรับสิทธิ์การเข้าถึงพิเศษและสร้างกลไกการอนุญาตที่เกี่ยวข้องในเวลาเดียวกัน Tencent Cloud ได้ปรับใช้เครื่องบินคุ้มกัน อย่างเต็มที่ในสภาพแวดล้อมการผลิต โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบแบ็กเอนด์จากส่วนกลางผ่าน เครื่องบินคุ้มกัน การเข้าถึง เครื่องบินคุ้มกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติการอนุญาต เจ้าหน้าที่ปฏิบัติการภายในบางส่วนของ Tencent Cloud เท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบ เครื่องบินคุ้มกัน ต้องการการยืนยันตัวตนสองปัจจัย บันทึกการเข้าสู่ระบบและบันทึกการดำเนินการทั้งหมดถูกรวบรวมไปยังแพลตฟอร์มการจัดการบันทึก (log) ของ Tencent Cloud เพื่อเก็บรักษาในรูปแบบเข้ารหัส ผ่านเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติการและทีมตรวจสอบภายในจะทำการตรวจสอบบันทึก (log) เพื่อตรวจจับความผิดปกติของระบบหรือการดำเนินการ เพื่อป้องกันความเสี่ยงในการปฏิบัติการ
6	การควบคุมการเข้ารหัส	ผู้ประกอบการธุรกิจต้องจัดให้มีการควบคุมการเข้ารหัสที่เชื่อถือได้และเป็นไปตามมาตรฐานสากล โดยกำหนดวิธีการเข้ารหัสข้อมูล (encryption) และการบริหารจัดการกุญแจเข้ารหัส (key management) อย่างปลอดภัยเพื่อให้มั่นใจได้ว่า	ลูกค้าควรใช้อัลกอริทึมการเข้ารหัสตามมาตรฐานสากล และสร้างนโยบาย มาตรฐาน และขั้นตอนการจัดการคีย์รหัสผ่านที่ครอบคลุมขั้นตอนต่างๆ เช่น การสร้าง การแจกจ่าย การติดตั้ง การอัปเดต การเพิกถอน การกู้คืน และการหมดอายุของคีย์รหัสผ่าน นอกจากนี้ ลูกค้าควรกำหนดมาตรการควบคุมสำหรับคีย์รหัสผ่านที่จัดเตรียมโดยบุคคลภายนอกให้ชัดเจน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		การอ้างไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความถูกต้องแท้จริง (authenticity) ของข้อมูลมีความเหมาะสมและมีประสิทธิภาพ ดังนี้	และจัดทำขั้นตอนการจัดการเหตุการณ์การรั่วไหลของ คีย์รหัสผ่าน
		6.1 กำหนดวิธีการเข้ารหัสที่ปลอดภัย	เพื่อให้แน่ใจในความเป็นความลับและความสมบูรณ์ ของข้อมูลลูกค้า ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการ ของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสานรวม Key Management Service (KMS)
		6.2 กำหนดการบริหารจัดการกุญแจและ เข้ารหัส โดยจัดให้มีมาตรการการควบคุมตั้งแต่ การสร้างและติดตั้ง กุญแจเข้ารหัส การจัดเก็บและสำรองกุญแจเข้ารหัส ไปจนถึงการเพิกถอนหรือทำลายกุญแจ และเข้ารหัส	เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล ในกระบวนการใช้อัลกอริธึมการเข้ารหัสระหว่างการถ่ายโอนและการจัดเก็บข้อมูล Tencent Cloud กำหนดให้ทีมงานภายในปฏิบัติตามมาตรฐานหรือกฎระเบียบที่เกี่ยวข้องกับการจัดการรหัสผ่านสากล เลือกใช้อัลกอริธึมระดับความปลอดภัยสูง เช่น AES-256
		6.3 กำหนดมาตรการการควบคุมกุญแจ และเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบ เพื่อให้มั่นใจได้ว่ากุญแจและการเข้ารหัสที่ สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคล อื่น	และให้แน่ใจว่าความยาวของคีย์เป็นไปตามข้อกำหนด การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API
		6.4 กำหนดกระบวนการรองรับกรณีเกิด การรั่วไหลของกุญแจเข้ารหัส	ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจก็มีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับ ธุรกิจของลูกค้า
			ในด้านการจัดการคีย์ ลูกค้าสามารถใช้ Key Management Service (KMS) KMS รองรับให้ลูกค้าสร้างและจัดการคีย์ได้อย่างง่ายดาย ตอบสนองความต้องการในการจัดการคีย์สำหรับแอปพลิเคชันและธุรกิจหลายรายการของลูกค้า และสอดคล้องกับข้อกำหนดด้านกฎระเบียบและการปฏิบัติตาม KMS รองรับการรวมเข้ากับคุณลักษณะการเข้ารหัสของบริการต่างๆ เช่น Object Storage, Distributed Database, Cloud Block Storage ได้อย่างราบรื่น เพื่อให้ลูกค้านำไปใช้ได้อย่างง่ายดาย ระบบการจัดการคีย์ใช้ Hardware Security Module (HSM) ที่ได้รับการรับรอง FIPS-140-2

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ในการสร้างและปกป้องคีย์ ใช้โปรโตคอลการส่งข้อมูลที่ปลอดภัย ใช้การปรับใช้ธุรกิจแบบกระจายคลัสเตอร์หลายศูนย์ข้อมูลและการสำรองข้อมูลออนไลน์ อุปกรณ์ HSM ชั้นล่างใช้การปรับใช้การสำรองข้อมูลแบบออฟไลน์ในศูนย์ข้อมูลสองแห่ง เพื่อให้มั่นใจในความพร้อมใช้งานสูงของระบบการจัดการคีย์ เพื่อรับประกันความปลอดภัยของข้อมูลที่ถูกเข้ารหัสและลดความเสี่ยงจากการถูกโจมตีหรือใช้ในทางที่ผิดของคีย์ KMS รองรับการหมุนเวียนคีย์เป็นระยะ และหลังการหมุนเวียนคีย์ยังคงเข้ากันได้กับข้อมูลที่ถูกเข้ารหัสก่อนการหมุนเวียน โดยไม่ส่งผลกระทบต่อการใช้งานของธุรกิจผู้ใช้ KMS ใช้วิธีการลบคีย์ที่หมดอายุ ถูกยกเลิกหรือรั่วไหลออกไปอย่างปลอดภัยและเชื่อถือได้ คีย์ที่ถูกลบไปแล้วไม่สามารถกู้คืนได้ และข้อมูลที่ถูกเข้ารหัสด้วยคีย์ดังกล่าวก็จะไม่สามารถถอดรหัสได้เช่นกัน สำหรับสถาบันในภาคการเงินที่ข้อมูลการสื่อสารและการจัดเก็บมีมูลค่าสูงและมีความลับสูง KMS ให้บริการการเข้ารหัส การปกป้องคีย์ และการจัดการสิทธิ์สำหรับเนื้อหาการสื่อสารตามข้อตกลง ไฟล์สำคัญ และข้อมูลสำคัญผ่านการเข้ารหัสแบบซองจดหมาย (envelope encryption) เพื่อให้เป็นไปตามข้อกำหนดด้านความปลอดภัยและการปฏิบัติตาม กระบวนการส่งและกระจายคีย์ได้รับการปกป้องด้วยการเข้ารหัส โดยเปิดใช้งาน TLSv1.2 เพื่อป้องกันการดักจับและการขโมยข้อมูลโดยบุคคลที่สาม (man-in-the-middle attacks) Tencent Cloud ยังได้กำหนดมาตรฐานการเข้ารหัสและการจัดการคีย์ โดยกำหนดข้อกำหนดด้านความปลอดภัยสำหรับกระบวนการต่างๆ ในการสมัครคีย์ การสร้าง การจัดเก็บ การใช้ การส่งต่อ การอัปเดต และการทำลายคีย์ การดำเนินการต่างๆ ที่เกี่ยวข้องกับวงจรชีวิตของคีย์ทั้งหมดต้องปฏิบัติตามข้อกำหนดพื้นฐานของการควบคุมสองชั้น การส่งมอบที่เข้มงวด การเก็บรักษาที่เหมาะสม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และการอัปเดตที่ทันทางที่ กระบวนการใช้ตัวยังต้องแน่ใจว่าปฏิบัติตามข้อกำหนด เช่น การแยกหน้าที่และความรับผิดชอบ การอนุมัติที่เข้มงวด และการดำเนินการด้วยข้อจริง และต้องเก็บรักษาบันทึกการดำเนินการคีย์ทางธุรกิจ และดำเนินการตรวจสอบการดำเนินการเป็นประจำ
7	การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	ผู้ประกอบการต้องจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สิน ด้าน IT พร้อมทั้งมีระบบการป้องกัน และกระบวนการบำรุงรักษาฮาร์ดแวร์และระบบสาธารณูปโภค (facilities) ที่เกี่ยวข้องกับ IT เพื่อให้สามารถป้องกันความเสียหายต่อทรัพย์สินด้าน IT ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location)	ลูกค้าควรสร้างกลไกการควบคุมความปลอดภัยทางกายภาพและสิ่งแวดล้อมสำหรับสินทรัพย์เทคโนโลยีสารสนเทศ และดำเนินการกระบวนการป้องกันความปลอดภัยและการบำรุงรักษาเป็นประจำสำหรับอุปกรณ์ฮาร์ดแวร์และโครงสร้างพื้นฐานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจในความปลอดภัยของสินทรัพย์ โครงสร้างพื้นฐานของ Tencent Cloud มีการกระจายตัวอยู่ในหลายสถานที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) ภูมิภาค (region) แต่ละแห่งเป็นพื้นที่ทางภูมิศาสตร์อิสระ ในขณะที่โซนความพร้อมใช้งานแต่ละโซนเป็นโดเมนการบำรุงรักษาความล้มเหลวอิสระ และแต่ละโซนความพร้อมใช้งานถูกแยกจากกันทางกายภาพ ลูกค้าสามารถปรับใช้ข้อมูลและระบบในภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างยืดหยุ่นตามความต้องการในการพัฒนาธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติทางธุรกิจ ในด้านความปลอดภัยของสภาพแวดล้อมศูนย์ข้อมูล ศูนย์ข้อมูลทั้งหมดของ Tencent Cloud ทั่วโลกดำเนินการเลือกที่ตั้ง ก่อสร้าง หรือเช่าตามมาตรฐานสากลที่เกี่ยวข้องและข้อกำหนดความปลอดภัยในท้องถิ่น ทั้งระบบไฟฟ้าและระบบปรับอากาศของแต่ละศูนย์ข้อมูล ออกแบบด้วยความเสถียรสูงและแบบซ้ำซ้อนเต็มรูปแบบ ความล้มเหลวของจุดใดจุดหนึ่งจะไม่ส่งผลกระทบต่อความต่อเนื่องของไฟฟ้าและการระบายความร้อนของศูนย์ข้อมูล แต่ละศูนย์ข้อมูลติดตั้งระบบดับเพลิงครบถ้วน รวมถึงระบบตรวจจับไฟในพื้นที่จุดเฉพาะ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ระบบดับเพลิงอัตโนมัติ และอุปกรณ์ดับเพลิงด้วยมือสำหรับใช้ในกรณีฉุกเฉิน ภายในศูนย์ข้อมูลแต่ละแห่งติดตั้งพื้นป้องกันไฟฟ้าสถิต ตัวรับ และรางสายไฟทั้งหมดติดตั้งสายกราวด์เพื่อป้องกันความ เสียหายต่ออุปกรณ์จากไฟฟ้าสถิต ในด้านการควบคุมการเข้าถึงศูนย์ข้อมูล Tencent Cloud ได้กำหนดขั้นตอนการเข้าถึงที่เป็นทางการสำหรับการเ เข้าถึงทางกายภาพของศูนย์ข้อมูล บุคคลที่ต้องการเข้าสู่ศูนย์ข้อมูลต้องแสดงตัวตนและนำ หลักฐานแสดงตัวตนมายื่นต่อเจ้าหน้าที่ปฏิบัติการควา มปลอดภัย ผู้จัดการศูนย์ข้อมูลแต่ละแห่งต้องบันทึกและจัดการการ มอบสิทธิ์ การแก้ไข และการยกเลิกสิทธิ์การเข้าถึงในระบบการเข้าถึงศูนย์ขั อมูลภายในของตน ผู้จัดการศูนย์ข้อมูลจะทบทวนสิทธิ์การเข้าถึงศูนย์ข้อมู ลเป็นประจำ เพื่อให้มั่นใจว่าการจัดสรรสิทธิ์การเข้าถึงอย่างเหมาะสม หากสิทธิ์การเข้าถึงไม่เกี่ยวข้องหรือไม่จำเป็นอีกต่อไป ผู้จัดการศูนย์ข้อมูลของ Tencent Cloud จะปิดการใช้งานสิทธิ์การเข้าถึงดังกล่าว ผู้เยี่ยมชมที่ได้รับอนุมัติให้เข้าสู่ศูนย์ข้อมูลของ Tencent Cloud ล้วนได้รับการดูแลโดยวิศวกรภาคสนามของ Tencent Cloud ผู้เยี่ยมชมหรือพนักงานทุกประเภทที่เข้าออกศูนย์ข้อมูล ต้องได้รับการตรวจสอบตัวตนและตรวจสอบสัมภาระที่ พกพา และลงทะเบียนสิ่งของที่นำติดตัวมา ในด้านการตรวจสอบและเฝ้าระวังศูนย์ข้อมูลและ การตรวจสอบประจำวัน การจัดการการเฝ้าระวังศูนย์ข้อมูลของ Tencent Cloud ครอบคลุมพื้นที่ภายในห้องเซิร์ฟเวอร์แต่ละแห่ง พื้นที่ส่งมอบงาน จุดเข้าออกพื้นที่ศูนย์ข้อมูล และจุดเข้าออกอาคารต่างๆ ภายในพื้นที่ศูนย์ข้อมูล ซึ่งทั้งหมดติดตั้งระบบแจ้งเตือนการเฝ้าระวังด้วยวิดีโอแ บบไม่มีจุดบอด 24 ชั่วโมงตลอด 7 วัน และมีเจ้าหน้าที่รักษาความปลอดภัยประจำการ 24 ชั่วโมงตลอด 7 วัน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เจ้าหน้าที่รักษาความปลอดภัยของศูนย์ข้อมูลแต่ละแห่งของ Tencent Cloud ดำเนินการตรวจสอบสถานการณ์ของห้องเซิร์ฟเวอร์และอุปกรณ์ต่างๆ อย่างเคร่งครัดตามรายการตรวจสอบและแผนการตรวจสอบ โดยครอบคลุมพื้นที่ต่างๆ เช่น จุดเข้าออกอาคาร บริเวณรอบอาคาร และภายในอาคาร พร้อมทั้งลงนาม ณ จุดตรวจและบันทึกเวลาในการตรวจสอบ ทันทีที่พบความขัดข้องของโครงสร้างพื้นฐานหรือเหตุการณ์ด้านความปลอดภัย จะเริ่มต้นขั้นตอนการตอบสนองเหตุฉุกเฉินของศูนย์ข้อมูลทันที ในด้านการฝึกซ้อมความปลอดภัยทางกายภาพของศูนย์ข้อมูล ศูนย์ข้อมูลแต่ละแห่งได้กำหนดแผนการตอบสนองฉุกเฉินด้านความปลอดภัยทางกายภาพ และจัดให้เจ้าหน้าที่ศูนย์ข้อมูลฝึกซ้อมด้านความปลอดภัยเป็นประจำ ทันทีที่เกิดเหตุการณ์ด้านความปลอดภัยทางกายภาพ แผนดังกล่าวจะมีผลบังคับใช้ทันทีและชี้แนะผู้เกี่ยวข้องให้ปกป้องสินทรัพย์ของลูกค้านำได้มากที่สุดเท่าที่จะเป็นไปได้ เหตุการณ์ด้านความปลอดภัยทั้งหมดจะถูกบันทึกและวิเคราะห์โดยละเอียด เพื่อใช้ในการปรับปรุงและยกระดับมาตรฐานและระบบการจัดการความปลอดภัยที่มีอยู่อย่างต่อเนื่อง นอกจากนี้ Tencent Cloud ยังดำเนินการตรวจสอบและตรวจสอบศูนย์ข้อมูลภาคสนามเป็นประจำ เพื่อให้แน่ใจว่าศูนย์ข้อมูลเป็นไปตามข้อกำหนดด้านความปลอดภัยข้อมูลที่ Tencent Cloud กำหนด Tencent Cloud ทบทวนผลการประเมินความเสี่ยงด้านภัยคุกคามและช่องโหว่ (TVRA) ที่ดำเนินการโดยผู้ให้บริการศูนย์ข้อมูล เพื่อให้มั่นใจในประสิทธิภาพของมาตรการจัดการที่เกี่ยวข้อง
8.1	การบริหารจัดการการตั้งค่าระบบ	โดยมีกระบวนการในการควบคุมการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่างถูกต้อง	ลูกค้าควรสร้างกลไกการจัดการการกำหนดค่าระบบ ทบทวนการกำหนดค่าระบบเป็นประจำเพื่อให้มั่นใจในความปลอดภัยและความถูกต้องของการกำหนดค่า Cloud Security Center (CSC)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		อง และปลอดภัย	ให้ฟังก์ชันการตรวจสอบและประเมินความเสี่ยงการกำหนดค่าผลิตภัณฑ์คลาวด์โดยอัตโนมัติ ช่วยลูกค้าลดความเสี่ยงด้านความปลอดภัยที่เกิดจากข้อผิดพลาดในการกำหนดค่าความปลอดภัยในการใช้ผลิตภัณฑ์คลาวด์ และยกระดับความปลอดภัยโดยรวมบนคลาวด์ในเวลาเดียวกัน ลูกค้าสามารถใช้ Config เพื่อดำเนินการตรวจสอบและควบคุมทรัพยากรคลาวด์จากส่วนกลาง บันทึกข้อมูลการกำหนดค่าและการเปลี่ยนแปลงการกำหนดค่าของทรัพยากรคลาวด์ต่างๆ ในภูมิภาคต่างๆ ภายใต้บัญชีของลูกค้าอย่างต่อเนื่อง และอิงตามกฎข้อปฏิบัติที่ดีที่สุดและเทมเพลตแพ็คเกจการปฏิบัติตามข้อกำหนดของ Tencent Cloud เพื่อประเมินความสอดคล้องของการกำหนดค่าทรัพยากรคลาวด์ภายใต้บัญชีองค์กรอย่างต่อเนื่องโดยอัตโนมัติ และระบุการกำหนดค่าทรัพยากรที่ไม่สอดคล้องเพื่อให้บรรลุการตรวจสอบและจัดการทรัพยากรคลาวด์โดยอัตโนมัติ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างระบบการจัดการการกำหนดค่าและบริหารจัดการส่วนประกอบบริการเทคโนโลยีสารสนเทศและรายการกำหนดค่าต่างๆ อย่างเป็นเอกภาพผ่านฐานข้อมูลการจัดการการกำหนดค่า รวมถึงควบคุมการจัดการรายการกำหนดค่า (CI) และความสัมพันธ์ระหว่างรายการดังกล่าว หากกระบวนการเปลี่ยนแปลงเกี่ยวข้องกับการอัปเดตการกำหนดค่า เจ้าหน้าที่ปฏิบัติการจะอัปเดตรุ่นและข้อมูลที่เกี่ยวข้องของรายการกำหนดค่าลงในฐานข้อมูลการจัดการการกำหนดค่าตามแผนการเปลี่ยนแปลง หลังจากดำเนินการเปลี่ยนแปลงเสร็จสิ้น Tencent Cloud จะตรวจนับสินทรัพย์เป็นประจำ และตรวจสอบฐานข้อมูลการจัดการการกำหนดค่าเพื่อให้มั่นใจในประสิทธิภาพ ความถูกต้อง และความสมบูรณ์ของข้อมูลรายการกำหนดค่าต่างๆ เพื่อให้สอดคล้องกับข้อกำหนดการกำกับดูแลของลูกค้า Tencent Cloud ได้กำหนดมาตรฐานการกำหนดค่าความปลอดภัยเครือข่ายและมาตรฐานเส้นฐานความปลอดภัยขึ้น

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
8.2	การบริหารจัดการการเปลี่ยนแปลง	อย่างรัดกุมเพียงพอ เพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต	เพื่อจัดการมาตรฐานการกำหนดค่าความปลอดภัยของอุปกรณ์เครือข่าย ไฟร์วอลล์ ระบบปฏิบัติการของเซิร์ฟเวอร์โฮสต์ ฐานข้อมูล และระบบแอปพลิเคชัน Tencent Cloud ใช้เครื่องมือสแกนเพื่อตรวจจับความเบี่ยงเบนของการกำหนดค่าระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และอิมเมจเสมือน (Virtual Image) จากมาตรฐานอย่างต่อเนื่อง สำหรับความเบี่ยงเบนที่ตรวจพบ Tencent Cloud จะสร้างใบงานความปลอดภัยและส่งไปยังทีมงานผู้รับผิดชอบโดยอัตโนมัติ เพื่อดำเนินการแก้ไขทันทีที่ Tencent Cloud ยังทบทวนนโยบายความปลอดภัยและการตั้งค่าพารามิเตอร์ของอุปกรณ์เครือข่าย เช่น เราเตอร์ ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย เป็นระยะ เพื่อให้มั่นใจในประสิทธิผลของนโยบายและพารามิเตอร์
			ลูกค้าควรกำหนดขั้นตอนการจัดการการเปลี่ยนแปลง ใช้มาตรการเฝ้าระวังที่มีประสิทธิภาพสำหรับการเปลี่ยนแปลงระบบ โดยการเปลี่ยนแปลงใดๆ ต้องได้รับการอนุญาตก่อนจึงจะดำเนินการได้ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานการจัดการสำหรับการเปลี่ยนแปลงผลิตภัณฑ์และการกำหนดค่าที่กำหนดขั้นตอนต่างๆ ในกระบวนการเปลี่ยนแปลงและผู้รับผิดชอบที่เกี่ยวข้องอย่างชัดเจน เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการอนุมัติและทดสอบอย่างเหมาะสมก่อนการดำเนินการ ในเวลาเดียวกัน Tencent Cloud ได้กำหนดขั้นตอนการจัดการสำหรับการเปลี่ยนแปลงฉุกเฉิน โดยการเปลี่ยนแปลงฉุกเฉินต้องได้รับการอนุมัติที่เหมาะสมก่อนจึงจะสามารถดำเนินการได้ การเปลี่ยนแปลงโปรแกรมทุกประเภท รวมถึงการเปลี่ยนแปลงแอปพลิเคชันและไฟล์กำหนดค่า ระบบปฏิบัติการ และฐานข้อมูล ต้องได้รับการวิเคราะห์ผลกระทบทางธุรกิจก่อนการเปิดตัว จัดทำแผนย้อนกลับสำหรับการเปลี่ยนแปลง และได้รับการอนุมัติจากผู้รับผิดชอบที่เกี่ยวข้อง ระบบเผยแพร่การเปลี่ยนแปลงของ Tencent Cloud บังคับให้การดำเนินการเปลี่ยนแปลงสามารถดำเนินการ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น และเก็บรักษานันทิกที่เกี่ยวข้องกับการเปลี่ยนแปลงไว้ พร้อมทั้งตรวจสอบบันทึกเป็นประจำ หลังการเผยแพร่การเปลี่ยนแปลง Tencent Cloud จะตรวจสอบ ตรวจสอบ และบันทึกผลการเปลี่ยนแปลงในสภาพแวดล้อมการผลิต Tencent Cloud จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอการดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน และขอบเขตของการเปลี่ยนแปลง สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแวดล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขยาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม
8.3	การบริหารจัดการ การขีดความสามารถของระบบ	โดยจัดให้มีมาตรฐานและ วิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานข องระบบ และการประเมินแนวโน้ม การใช้ทรัพยากรด้าน IT เพื่อให้สามารถรองรับการดำเนินธุรกิจ ในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากร ให้รองรับการใช้งานในอนาคตได้อย่าง มีประสิทธิภาพ	ลูกค้าควรเฝ้าติดตามการใช้ทรัพยากรระบบอย่างต่อเนื่อง กำหนดขีดจำกัดประสิทธิภาพและความจุ และดำเนินการตามการที่จำเป็นเพื่อจัดการกับสถานการณ์ที่เกินขีดจำกัดที่กำหนดไว้ล่วงหน้า วางแผนทรัพยากรเพื่อให้สอดคล้องกับความต้องการในการใช้ในอนาคต เพื่อสนับสนุนลูกค้าในการวางแผนและปรับขนาดความ จุอย่างสะดวก Tencent Cloud ให้บริการ Auto Scaling (AS) สามารถตรวจจับสถานะสุขภาพของอินสแตนซ์โดยอัตโนมัติ และปรับทรัพยากรการคำนวณของเซิร์ฟเวอร์คลาวด์โดยอัตโนมัติตามความต้องการทางธุรกิจ นโยบาย และเงื่อนไขการขยายและลดขนาดที่กำหนดไว้ล่วงหน้า ของลูกค้า เพื่อให้แน่ใจว่ามีอินสแตนซ์เซิร์ฟเวอร์คลาวด์ที่เพียงพอ เสมอในการประมวลผลโหลดของแอปพลิเคชันของลูกค้า า เพื่อให้บรรลุการตรวจสอบและจัดการประสิทธิภาพของ ระบบ ลูกค้าสามารถใช้ Tencent Cloud Observability Platform (TCOP) ซึ่งให้บริการตรวจสอบแบบเรียลไทม์ การวิเคราะห์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และการแจ้งเตือนสำหรับผลิตภัณฑ์/ทรัพยากรคลาวด์ รวบรวมและแสดงตัวชี้วัดการตรวจสอบต่างๆ ที่รายงานโดยผลิตภัณฑ์คลาวด์ เช่น เซิร์ฟเวอร์คลาวด์และฐานข้อมูลคลาวด์ รวมถึงตัวชี้วัดการตรวจสอบที่กำหนดเองและรายงานโด ยลูกค้าผ่านแดชบอร์ดที่มองเห็นได้ ช่วยให้ลูกค้าติดตามอัตราการใช้ทรัพยากรผลิตภัณฑ์คล 라우드 ประสิทธิภาพของแอปพลิเคชัน และสถานะการทำงานของผลิตภัณฑ์คลาวด์แบบเรียลไ ทม์ และสนับสนุนการตั้งค่าการแจ้งเตือนตามตัวชี้วัด โดยแจ้งให้ลูกค้าทราบถึงความผิดปกติของธุรกิจอย่าง ทันทั่วทั้งผ่านการส่งข้อความและช่องทางอื่นๆ ตามกฎหมายการแจ้งเตือนที่ตั้งไว้ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำ กับดูแล Tencent Cloud ทำการคาดการณ์ความต้องการด้านความจุตามความ ต้องการในการดำเนินงานทางธุรกิจ และจัดทำแผนการจัดการความจุประจำปี ฝ่ายธุรกิจในขณะที่รับประกันความต่อเนื่องทางธุรกิจข องระบบสารสนเทศ อ้างอิงแนวโน้มการใช้ความจุที่ได้รับจากการตรวจสอบ ก่อนหน้าและคำนึงถึงความต้องการของธุรกิจและระบบใ หม์ ทำการคาดการณ์ความจุและวางแผนความจุ ในกระบวนการดำเนินงานประจำวัน ทีมงานภายใน Tencent Cloud ตรวจสอบการใช้ความจุของบริการสนับสนุนพื้นฐานข องแพลตฟอร์มคลาวด์แบบเรียลไทม์ผ่านแพลตฟอร์มต รวจสอบความจุภายใน และระบุแนวโน้มการใช้ความจุ เมื่อการใช้เกินขีดจำกัดที่กำหนดไว้ แพลตฟอร์มตรวจสอบจะแจ้งเตือนทีมงานที่เกี่ยวข้องให้ ติดตามและดำเนินการที่เหมาะสม เพื่อให้แน่ใจว่าผลิตภัณฑ์และบริการทำงานอย่างราบรื่น
8.4	การรักษาความ มั่นคงปลอดภัยของเครื่อง แม่ข่าย (server) และอุปกรณ์ที่ ใช้ปฏิบัติงาน (endpoint)	ให้สามารถป้องกันการโจมตีด้วยรูปแบบ ต่างๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) เพื่อลดความเสี่ยง จากการถูกโจมตีระบบ IT ขององค์กร หรือถูกใช้เป็นช่องทางในการโจมตีหน่ว งานอื่น และป้องกันการรั่วไหล ของข้อมูลสำคัญหรือการเข้าใช้งานระ บบ IT โดยไม่ได้รับอนุญาต	ลูกค้าควรรักษามาตรการป้องกันบนอุปกรณ์ปลายทาง โดยปรับใช้ซอฟต์แวร์ป้องกันไวรัสเพื่อสแกนระบบเป็นป ระจํา และอัปเดตฐานข้อมูลไวรัสอย่างทันทั่วทั้ง เพื่อให้สามารถเฝ้าระวังและระบุกิจกรรมที่ผิดปกติบนระ บบปลายทาง ลูกค้าสามารถใช้ Cloud Workload Protection Platform (CWPP) ใช้ข้อมูลภัยคุกคามจำนวนมากมหาศาลที่รวบรวมสะสมมา โดยใช้การเรียนรู้ของเครื่อง (Machine Learning)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อให้บริการป้องกันความปลอดภัยแก่ลูกค้า เช่น การตรวจจับการบุกรุกของแฮกเกอร์ การแจ้งเตือนความเสี่ยงจากช่องโหว่ รวมถึงฟังก์ชันความปลอดภัยต่าง ๆ เช่น การบล็อกการถอดรหัสผ่าน การแจ้งเตือนการเข้าสู่ระบบที่ผิดปกติ การตรวจจับไฟล์มัลแวร์โทรจัน การตรวจจับช่องโหว่ที่มีความเสี่ยงสูง เพื่อแก้ไขความเสี่ยงด้านความปลอดภัยเครือข่ายหลัก ที่เซิร์ฟเวอร์กำลังเผชิญอยู่ในปัจจุบัน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการป้องกันอุปกรณ์ปลายทางของโฮสต์ Tencent Cloud ได้ปรับใช้เครื่องมือตรวจจับและตอบสนองจุดปลายทาง (EDR) เพื่อตรวจสอบและควบคุมสินทรัพย์อุปกรณ์ปลายทางของเซิร์ฟเวอร์ทั่วทั้งเครือข่ายอย่างครอบคลุม เครื่องมือ EDR ที่ Tencent Cloud ใช้สนับสนุนการป้องกันไวรัสและการตรวจจับการบุกรุก เส้นฐานความปลอดภัยและการสแกนช่องโหว่ รวมถึงการตรวจสอบความสอดคล้องด้านความปลอดภัยสำหรับการดำเนินการคำสั่งและพฤติกรรมการเข้าสู่ระบบ และจะทริกเกอร์การแจ้งเตือนเมื่อตรวจพบโปรแกรมที่เป็นอันตรายหรือพฤติกรรมที่ผิดปกติ Tencent Cloud ติดตามและจัดการเหตุการณ์แจ้งเตือนผ่านระบบในงาน ในด้านการป้องกันอุปกรณ์ปลายทางในที่ทำงาน Tencent Cloud ได้กำหนดมาตรฐานความปลอดภัยของซอฟต์แวร์ภายในองค์กร ซึ่งกำหนดขีดจำกัดในการใช้ซอฟต์แวร์บนอุปกรณ์ปลายทางในที่ทำงาน (รวมถึงแล็ปท็อปและเวิร์กสเตชัน) และใช้เทคโนโลยีไวท์ลิสต์แอปพลิเคชัน อนุญาตให้รันเฉพาะโปรแกรมที่รู้จักและเชื่อถือได้เท่านั้น เพื่อลดความเสี่ยงจากการบุกรุกของซอฟต์แวร์ที่เป็นอันตราย Tencent Cloud ยังควบคุมอุปกรณ์ปลายทางผ่านระบบจัดการความปลอดภัยแบบ Zero-Trust โดยใช้ความสามารถด้านความปลอดภัย เช่น

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			การกำจัดไวรัส การแก้ไขช่องโหว่ และการป้องกันเชิงรุก เพื่อให้บรรลุการป้องกันความปลอดภัยรอบด้าน เช่น การป้องกันแรนซัมแวร์ การป้องกันการฟิชซิง การป้องกันการเคลื่อนย้ายภายใน เป็นต้น
8.5	กลยุทธ์และมาตรการความปลอดภัยในการทำงานระยะไกล	การกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และรวมถึงการใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) โดยพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมอย่างเหมาะสม	ลูกค้าควรควบคุมความปลอดภัยสำหรับการทำงานระยะไกล การใช้อุปกรณ์เคลื่อนที่ และการนำอุปกรณ์ส่วนตัวมาใช้ (BYOD) เพื่อป้องกันความเสี่ยงด้านความปลอดภัยที่เกิดจากการใช้ที่ไม่เหมาะสมของอุปกรณ์เคลื่อนที่ เพื่อความสะดวกของลูกค้าในการเข้าถึงระบบธุรกิจบนคลาวด์ได้อย่างปลอดภัยและรวดเร็ว ทุกเวลา ทุกสถานที่ และโดยใช้อุปกรณ์ปลายทางหลักใดๆ ก็ตาม Tencent Cloud รองรับเทคโนโลยีการเข้าถึงระยะไกล SSL VPN SSL VPN สามารถปกป้องความปลอดภัยของข้อมูลที่ส่งผ่านอินเทอร์เน็ตด้วยวิธีการเข้ารหัส และยังสามารถรองรับการควบคุมการเข้าถึงที่เหมาะสม เพื่อลดการเข้าถึงโดยไม่ได้รับอนุญาต ลูกค้ายังสามารถใช้ VPN Connection เพื่อให้บรรลุการส่งข้อมูลระหว่างศูนย์ข้อมูลในพื้นที่และทรัพยากรบน Tencent Cloud ภูมิภาค VPN ใช้ IKE (โปรโตคอลแลกเปลี่ยนคีย์ลับ) และ IPsec เพื่อเข้ารหัสข้อมูลที่ส่ง สร้างอุโมงค์ข้อมูลที่ปลอดภัยและนำเชื่อถือบนอินเทอร์เน็ต เพื่อปกป้องความปลอดภัยของข้อมูลระหว่างการส่ง VPN Gateway มีความน่าเชื่อถือสูง โดยใช้สถาปัตยกรรมการสำรองข้อมูลออนไลน์แบบสองเครื่องที่ระดับล่าง เพื่อรับประกันว่าการสื่อสารเซสชันจะไม่ขาดตอน และแอปพลิเคชันระดับบนไม่รู้สึกถึงความเปลี่ยนแปลง สำหรับการเข้าถึงระยะไกล Tencent Cloud ได้สร้างขั้นตอนการจัดการการเข้าถึงระยะไกลของพนักงานภายใน โดยพนักงานสามารถใช้อุปกรณ์ที่เชื่อถือได้ซึ่งลงทะเบียนกับ Tencent Cloud แล้วเท่านั้น และเข้าถึงเครือข่ายสำนักงานและระบบงานประจำวันของ Tencent Cloud ทางไกลผ่านช่องทางการสื่อสารที่เข้ารหัส Tencent Cloud จะบำรุงรักษาบันทึกการเข้าถึงระยะไกล

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และบันทึกพฤติกรรมการดำเนินการของผู้ใช้ ในเวลาเดียวกัน เครือข่ายสำนักงานภายในของ Tencent Cloud และสภาพแวดล้อมการผลิตที่ข้อมูลลูกค้าอยู่นั้นถูกแยก จากกันโดยสมบูรณ์ เมื่อพนักงานของ Tencent Cloud ได้รับความยินยอมและการอนุญาตจากลูกค้าให้เข้าถึง สินทรัพย์ข้อมูลของลูกค้า ต้องเข้าถึงสภาพแวดล้อมการผลิตที่ข้อมูลลูกค้าอยู่ผ่าน น เครื่องบินคุ้มกัน และบัญชีการปฏิบัติงานทั้งหมดมีการติดตั้งกลไกการยืนยันตัวตนสองปัจจัย ในด้านการใช้และการจัดการอุปกรณ์เคลื่อนที่ Tencent Cloud ได้กำหนดมาตรฐานการจัดการความปลอดภัยในการ ทำงานระยะไกลด้วยอุปกรณ์เคลื่อนที่ ซึ่งกำหนดมาตรฐานการใช้ที่ปลอดภัยสำหรับอุปกรณ์เคลื่อนที่ภายในและการรับประกันความปลอดภัยข้อมูล สำหรับแอปพลิเคชันการทำงานระยะไกล เมื่อพนักงานใช้อุปกรณ์เคลื่อนที่ ต้องใช้อุปกรณ์เคลื่อนที่ที่จัดเตรียมให้โดยบริษัทอย่างเป็น มาตรฐานเท่านั้น และจำกัดการใช้อุปกรณ์ส่วนตัว (BYOD) มีเฉพาะอุปกรณ์เคลื่อนที่ที่ผ่านการรับรอง (รวมถึงต้องผ่านการรับรองที่เกี่ยวข้องในอุตสาหกรรม ข้อกำหนดเวอร์ชันระบบปฏิบัติการ ฯลฯ) และเป็นไปตามข้อกำหนดหน้าที่และบทบาทของผู้ใช้ หลังจากได้รับอนุญาตที่สอดคล้องกันก่อนการใช้ จึงจะสามารถใช้งานได้ โดยปราศจากการอนุญาต จะไม่สามารถใช้อุปกรณ์เคลื่อนที่ส่วนตัวเชื่อมต่อกับอุปกรณ์สำนักงานโดยพลการได้ Tencent Cloud ได้ปรับใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust เพื่อควบคุมความปลอดภัย โดยใช้ความสามารถด้านความปลอดภัยของระบบจัดการ ความปลอดภัยแบบ Zero-Trust เช่น การกำจัดไวรัส การแก้ไขช่องโหว่ และการป้องกันเชิงรุก เพื่อให้บรรลุการป้องกันความปลอดภัยรอบด้าน เช่น การป้องกันแรนซัมแวร์ การป้องกันการฟิชชิ่ง และการป้องกันการเคลื่อนย้ายภายใน ระบบจัดการความปลอดภัยแบบ Zero-Trust

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
8.6	การสำรองข้อมูล	ที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีประสิทธิภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบ IT ในกรณีที่เกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง	ยังรองรับฟังก์ชันการตรวจสอบการส่งข้อมูลที่ละเอียดอ่อนนอกสูกายนอก ซึ่งสามารถตรวจสอบและบล็อกพฤติกรรมกรรมการส่งไฟล์ออกผ่านทางช่องทางต่างๆ เช่น อีเมล Cloud storage การควบคุมระยะไกล และเครื่องมือถ่ายโอนไฟล์ เพื่อป้องกันกิจกรรมการขโมยข้อมูลที่มีศักยภาพ
			ลูกค้าควรสร้างกลไกการจัดการการสำรองข้อมูลสำรองข้อมูลสำคัญ และเข้ารหัสและปกป้องทางกายภาพสำหรับสื่อจัดเก็บข้อมูลสำรอง และดำเนินการทดสอบการกู้คืนจากการสำรองข้อมูลเป็นประจำ ภายในปี 2026 Tencent Cloud ได้ติดตั้งศูนย์ข้อมูลสามแห่งภายในประเทศไทย โดยแต่ละแห่งมีระบบไฟฟ้าและเครือข่ายที่ทำงานอิสระต่อกัน สามารถสนับสนุนให้ลูกค้าเก็บข้อมูล ประมวลผล และสำรองข้อมูลภายในประเทศได้ บริการจัดเก็บข้อมูลและบริการฐานข้อมูลหลายรายการที่ Tencent Cloud มอบให้ฟังก์ชันการสำรองข้อมูล พร้อมตอบสนองความต้องการสำรองข้อมูลทุกรูปแบบของลูกค้า ตัวอย่างเช่น: - ข้อมูลของลูกค้าเก็บไว้ใน Cloud Object Storage (COS) สามารถจัดเก็บข้อมูลในหลายพื้นที่ที่กำหนดพร้อมกันผ่านฟังก์ชันการทำสำเนาข้ามพื้นที่ เพื่อให้แน่ใจว่าแม้ในกรณีที่สูญเสข้อมูลบางส่วนไปโดยไม่ได้คาดหมาย ก็ยังสามารถค้นหาและกู้คืนข้อมูลทั้งหมดได้ผ่านข้อมูลสำรอง - และยังหลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้นเมื่อพื้นที่เก็บข้อมูลในโซนความพร้อมใช้งานหนึ่งประสบภัยพิบัติที่ไม่อาจหลีกเลี่ยงได้ - ซึ่งช่วยให้บรรลุผลสำรองข้อมูลหลายชุดและการกู้คืนจากภัยพิบัติข้ามพื้นที่ - ฟังก์ชันการสำรองข้อมูลแบบสแนปช็อตของ Cloud Block Storage (CBS) ทำการสำรองข้อมูลโดยการถ่ายสแนปช็อต ณ จุดเวลาใดเวลาหนึ่งของ CBS - ป้องกันการสูญเสข้อมูลเนื่องจากการแก้ไขโดยไม่ได้รับอนุญาตและการลบผิดพลาด

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และรับประกันความสามารถในการย้อนกลับอย่างรวดเร็วเมื่อเกิดความขัดข้องทางธุรกิจ • <u>Cloud File Storage (CFS)</u> ให้ฟังก์ชันสแนปช็อตเป็นระยะเพื่อความสะดวกในการตั้งค่านโยบายงานสำรองข้อมูลตามความยืดหยุ่นของลูกค้า • <u>Cloud Native Database TDSQL-C</u> รองรับการสำรองข้อมูลสองประเภท: การสำรองข้อมูลเชิงตรรกะและการสำรองข้อมูลแบบสแนปช็อต ด้วยการสำรองข้อมูลที่สมบูรณ์และการสำรองข้อมูล binlog ในช่วงเวลาต่อมา ทำให้สามารถกู้คืนคลัสเตอร์ TDSQL-C MySQL Edition ทั้งหมดหรือตารางฐานข้อมูลเฉพาะไปยังจุดเวลาใดก็ได้ • <u>TencentDB for MySQL</u> รองรับสองวิธีในการสำรองข้อมูลฐานข้อมูล: การสำรองข้อมูลอัตโนมัติและการสำรองข้อมูลด้วยตนเอง และให้ฟังก์ชันการสำรองข้อมูลข้ามพื้นที่เพื่อช่วยลูกค้าเพิ่มความสามารถในการกู้คืนจากภัยพิบัติและเพิ่มความน่าเชื่อถือของข้อมูลไปพร้อมๆ กัน • <u>TencentDB for MongoDB</u> ให้กลไกการสำรองข้อมูลอัตโนมัติและการกู้คืนโดยไม่สูญเสียข้อมูล รองรับการสำรองข้อมูลแบบหลายโหนด ลูกค้าสามารถเก็บข้อมูลสำรองไว้หลายวันผ่านกลไกการสำรองข้อมูล เพื่อความสะดวกในการกู้คืนข้อมูลในสถานการณ์ภัยพิบัติ
8.7	การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log)	อย่างครบถ้วนและเพียงพอเพื่อให้สามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและ ใช้งานข้อมูลและระบบ IT ย้อนหลังได้ ตามที่กฎหมายกำหนด	ลูกค้าควรรวบรวมและปกป้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศอย่างครอบคลุมและเพียงพอ เพื่อให้มั่นใจในความสมบูรณ์และการติดตามได้ของบันทึก (log) และดำเนินการตรวจสอบบันทึกสำหรับการเข้าถึงและการใช้ข้อมูลและระบบสารสนเทศเป็นประจำ เพื่อช่วยลูกค้าในกระบวนการรวบรวม สรุ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และวิเคราะห์บันทึก Tencent Cloud ให้บริการ Cloud Log Service (CLS) ซึ่งเป็นแพลตฟอร์มบริการบันทึกแบบครบวงจร CLS ให้บริการหลายรายการตั้งแต่การรวบรวมบันทึกการจัดเก็บบันทึก ไปจนถึงการสืบค้นและวิเคราะห์บันทึก การบริโภคแบบเรียลไทม์ และการส่งบันทึก ช่วยลูกค้าแก้ไขปัญหาต่างๆ เช่น การดำเนินงานทางธุรกิจ การตรวจสอบความปลอดภัย การตรวจสอบบันทึก และการวิเคราะห์บันทึก CLS ออกแบบด้วยสถาปัตยกรรมแบบกระจายที่มีความพร้อมใช้งานสูง จัดเก็บข้อมูลบันทึกด้วยการสำรองข้อมูลหลายชุด ป้องกันไม่ให้ข้อมูลไม่สามารถใช้งานได้เมื่อบริการไหนใดเดียวล้มเหลว บรรลุความพร้อมใช้งานสูงของบริการ และให้การรับประกันบริการที่เสถียรและเชื่อถือได้สำหรับข้อมูลบันทึก Cloud Security Center (CSC) ยังสนับสนุนการรวบรวมข้อมูลที่เกี่ยวข้องกับความปลอดภัยบนคลาวด์ประเภทต่างๆ เช่น ข้อมูลการแจ้งเตือนของผลิตภัณฑ์ความปลอดภัยคลาวด์ ข้อมูลการเปลี่ยนแปลงการกำหนดค่าสินทรัพย์คลาวด์ ข้อมูลพฤติกรรมกรรมการดำเนินการของผู้ใช้บนคลาวด์ และข้อมูลบันทึกของผลิตภัณฑ์คลาวด์บางส่วน และให้แพลตฟอร์มการสืบค้นและสอบสวนแบบครบวงจร ช่วยลูกค้าบรรลุการตรวจสอบบันทึกและการสืบค้นและสอบสวนบันทึกบนคลาวด์อย่างครอบคลุม นอกจากนี้ บริการ Elasticsearch Service (ES) จะรวบรวมและส่งบันทึกแบบเรียลไทม์ของเซิร์ฟเวอร์คลาวด์ คอนเทนเนอร์ และผลิตภัณฑ์คลาวด์อื่นๆ หรือข้อมูลธุรกิจที่มีอยู่และเพิ่มขึ้นของธุรกิจไปยังคลัสเตอร์ ES ของ Tencent Cloud เพื่อจัดเก็บข้อมูลแบบกระจาย และการสืบค้นและการวิเคราะห์ข้อมูล สำหรับการรวบรวมและการเก็บรักษาบันทึกเครือข่าย Cloud Firewall (CFW) รองรับการวิเคราะห์บันทึกเครือข่ายของปริมาณข้อมูลทั้งหมด และสามารถเก็บรักษาได้สูงสุด 6 เดือน และรองรับการวิเคราะห์การติดตามภัยคุกคามขั้นสูง ซึ่งสามารถวิเคราะห์ข้อมูลการจดทะเบียนโดเมน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			การแก้ไข การขึ้นทะเบียน และประวัติการแก้ไขได้ สำหรับการรวบรวมและการเก็บรักษาบันทึกการดำเนินการ ลูกค้าสามารถใช้ CloudAudit เพื่อกำกับดูแลกิจกรรมบัญชี Tencent Cloud ตรวจสอบความสอดคล้อง ตรวจสอบการดำเนินการ และตรวจสอบความเสี่ยง CloudAudit รองรับการดูบันทึกการดำเนินการของคอนโซล Tencent Cloud และ API คลาวด์ภายใน 90 วันออนไลน์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการจัดการบันทึก Tencent Cloud ได้สร้างมาตรฐานและกลไกการรวบรวมและการจัดการบันทึก เพื่อควบคุมการบันทึก การตั้งข้อมูล การจัดเก็บ การป้องกัน การวิเคราะห์ และการตรวจสอบบันทึกต่างๆ เช่น บันทึกการเข้าสู่ระบบ บันทึกการดำเนินการ บันทึกระบบทั่วไป และบันทึกเหตุการณ์ความปลอดภัยของระบบ เพื่อตรวจจับและป้องกันความผิดปกติและความเสี่ยงของกิจกรรมระบบ บันทึกทั้งหมดถูกรวมเข้าสู่แพลตฟอร์มการจัดการบันทึกของ Tencent Cloud เพื่อการจัดการ และมีการใช้มาตรการสำรองข้อมูลและการป้องกันที่เข้มงวดสำหรับข้อมูลบันทึกที่เกี่ยวข้อง เพื่อป้องกันการแก้ไขและการลบโดยไม่ได้รับอนุญาต Tencent Cloud ดำเนินการตรวจสอบบันทึกผ่านเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติการและทีมตรวจสอบภายใน เพื่อตรวจจับความผิดปกติของระบบหรือการดำเนินการ เพื่อป้องกันความเสี่ยงในการปฏิบัติการ
8.8	การติดตามดูแลระบบและฝ่ายระงับความเสียหายเบอร์ดอร์	โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ	ลูกค้าควรสร้างขั้นตอนหรือใช้เครื่องมือที่เกี่ยวข้องเพื่อตรวจสอบระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าสามารถค้นพบความผิดปกติหรือภัยคุกคามที่อาจส่งผลกระทบต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศที่สำคัญได้ทันเวลาที่ เพื่อสนับสนุนลูกค้าในการตรวจจับและวิเคราะห์ภัยคุกคาม Tencent Cloud ให้บริการ Threat Intelligence X (TIX) แก่ลูกค้า

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ซึ่งเป็นแพลตฟอร์มบริการชาวกรองแบบครบวงจร TIX สามารถให้ความสามารถด้านชาวกรองสามประเภทหลัก ได้แก่ ชาวกรองพื้นฐาน ชาวกรองด้านพื้นผิวการโจมตี และชาวกรองทางธุรกิจ รองรับฟังก์ชันต่างๆ เช่น การสืบค้นชาวกรอง การวิเคราะห์และประเมิน IOC การจัดการพื้นผิวการโจมตี สามารถช่วยลูกค้าวิเคราะห์และประเมินเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น และประเมินความเสี่ยงด้านการเปิดเผยสินทรัพย์ขององค์กรอย่างครอบคลุมมากขึ้น สนับสนุนองค์กรในการสร้างระบบป้องกันความปลอดภัยแบบสามมิติที่มีประสิทธิภาพ TIX สร้างเครือข่ายจุดสัมผัสชาวกรองที่สมบูรณ์ โดยรวบรวมและวิเคราะห์ชาวกรองภัยคุกคามจากแหล่งที่มาหลากหลาย เช่น ชุมชนช่องโหว่ องค์กรความปลอดภัย ผู้ผลิตเครื่องมือความปลอดภัย โซเชียลมีเดีย บล็อกความปลอดภัย และเชื่อมโยงกับอัลกอริธึมและพลังการคำนวณบนคลาวด์เพื่อจัดผลบวกปลอม ซึ่งรับประกันความแม่นยำของชาวกรอง นอกจากนี้ ศูนย์ชาวกรองภัยคุกคามใช้ SaaS เป็นแกนกลาง รองรับวิธีการส่งมอบต่างๆ เช่น API ผังเว็บ SDK TIP และ Mini Program เพื่อตอบสนองความต้องการที่หลากหลายของลูกค้า ศูนย์ชาวกรองภัยคุกคามยังสามารถบูรณาการกับผลิตภัณฑ์ป้องกันความปลอดภัยที่มีอยู่ของลูกค้าในรูปแบบการรวมเข้าด้วยกัน เพื่อเชื่อมโยงข้อมูลชาวกรองจากคลาวด์กับผลิตภัณฑ์ดังกล่าว เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัยโดยรวมและการตอบสนองต่อภัยคุกคาม ด้วยการเสริมพลังและการสนับสนุนจากศูนย์ชาวกรองภัยคุกคาม Tencent Cloud มุ่งมั่นที่จะสร้างระบบความสามารถด้านความปลอดภัยในการป้องกันเชิงรุกแบบ "ชาวกรอง-การโจมตีและการป้องกัน-การจัดการ-การวางแผน" โดยบูรณาการเทคโนโลยีต่างๆ เช่น ชาวกรองภัยคุกคาม ปัญญาประดิษฐ์ ข้อมูลขนาดใหญ่ เพื่อเพิ่มความสามารถและประสิทธิภาพในการตอบสนองต่อเหตุการณ์ความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และได้จัดตั้งศูนย์ปฏิบัติการความปลอดภัยที่ทำงาน 24 ชั่วโมงทุกวัน ให้ความสำคัญกับการตรวจจับภัยคุกคาม การสอบสวน และการตอบสนอง เพื่อให้บรรลุความสามารถในการรับรู้ มองเห็น และควบคุมสถานการณ์ความปลอดภัย
8.9	การประเมินช่องโหว่ทางเทคนิค	ของระบบ IT ที่เหมาะสมกับระดับความเสี่ยงเพื่อให้ทราบถึงช่องโหว่ และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันเวลาที่โดยการประเมินช่องโหว่ทางเทคนิคครอบคลุมระบบ IT ที่มีนัยสำคัญและระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) ทุกระบบอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบดังกล่าว	ลูกค้าควรดำเนินการประเมินช่องโหว่และการทดสอบเจาะระบบเป็นประจำ เพื่อระบุช่องโหว่ด้านความปลอดภัยและประเมินความสามารถในการป้องกันความปลอดภัยทางเครือข่าย และดำเนินการมาตรการแก้ไขและป้องกันภัยคุกคามความปลอดภัยทางเครือข่ายที่อาจเกิดขึ้นอย่างทันทางที่ นอกจากนี้ ลูกค้าควรให้มั่นใจว่าการบันทึกกิจกรรมการทดสอบเจาะระบบจะถูกเก็บรักษาไว้อย่างน้อยสองปี และเมื่อได้รับแจ้งจากหน่วยงานกำกับดูแล ควรส่งรายงานผลการทดสอบเจาะระบบทันที
8.10	การทดสอบการเจาะระบบ	8.10.1 ผู้ประกอบธุรกิจต้องจัดให้มีการทดสอบการเจาะระบบดังนี้ (1) ระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) (1.1) อย่างน้อยปีละ 1 ครั้ง และ (1.2) ทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ (2) ระบบอื่น ๆ นอกจาก (1) จัดให้มีการประเมินความเสี่ยงจากการบุกรุกผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้สื่อสารภายในองค์กรเพื่อกำหนดขอบเขตการทดสอบการเจาะระบบและทดสอบการเจาะระบบตามความเหมาะสม 8.10.2 การทดสอบการเจาะระบบข้างต้นต้องดำเนินการโดยผู้เชี่ยวชาญภายใน	ในการดำเนินการทดสอบเจาะระบบ Tencent Cloud ให้บริการ Penetration Testing Service (PTS) แก่ลูกค้า ด้วยการจำลองเทคนิคการโจมตีและเทคนิคการค้นพบช่องโหว่ที่แฮกเกอร์อาจใช้อย่างเต็มรูปแบบ ใช้วิธีการและกลไกที่ควบคุมได้และไม่ทำลายล้างเพื่อทำการตรวจสอบความปลอดภัยของระบบเป้าหมายอย่างลึกซึ้ง ค้นหาจุดอ่อนที่มีอยู่ในเป้าหมายและอุปกรณ์เครือข่าย ให้คำแนะนำในการเสริมความแข็งแกร่งด้านความปลอดภัยเพื่อช่วยลูกค้ายกระดับความปลอดภัยของระบบ และสนับสนุนการตรวจสอบหลังการแก้ไขช่องโหว่ ในการสแกนช่องโหว่ ลูกค้าสามารถเลือกใช้ Vulnerability Scanning Service (VSS) เพื่อตรวจสอบสินทรัพย์เครือข่ายขององค์กรและระบุความเสี่ยงของสินทรัพย์นั้นๆ โดยใช้ประโยชน์จากประสบการณ์ด้านความปลอดภัยและข่าวกรองภัยคุกคามที่สะสมมาหลายปีของ Tencent Cloud VSS ได้สร้างฐานข้อมูลกฎของโหว่ที่อุดมสมบูรณ์และครอบคลุม และมีความสามารถในการตรวจจับช่องโหว่ 0Day/1Day/NDay ที่มีอาชีวะและมีประสิทธิภาพสูง สามารถดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ในหรือภายนอก ที่เป็นอิสระจากเจ้าของระบบ	ความปลอดภัย และความสอดคล้องของสินทรัพย์ของลูกค้า
		8.10.3 ในกรณีที่มีการตรวจพบช่องโหว่ที่ผู้ประกอบธุรกิจต้องดำเนินการแก้ไขและป้องกัน ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นอย่างทันห่วงที่ เพื่อขจัดความเสี่ยงจากช่องโหว่ดังกล่าว	ให้คำแนะนำการแก้ไขที่มีอาชีวะแก่ลูกค้า เพื่อลดความเสี่ยงด้านความปลอดภัย VSS ยังสนับสนุนการทำงานร่วมกับผลิตภัณฑ์คลาวด์ เช่น ความปลอดภัยโฮสต์ไฟร์วอลล์แอปพลิเคชันเว็บ เพื่อให้บรรลุการปิดจากการตรวจสอบความเสี่ยงไปจนถึงการจัดการความเสี่ยง
		8.10.4 ผู้ประกอบธุรกิจต้องจัดเก็บรายงานการดำเนินการตามข้อ 8.10 เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำเอกสารนั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้ สำนักงานสามารถเรียกดูและตรวจสอบได้ โดยไม่ชักช้า	เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะสร้างงานสแกนเป็นประจำผ่านระบบสแกนช่องโหว่เพื่อ สแกนช่องโหว่ของสินทรัพย์ในสภาพแวดล้อมคลาวด์ และวิเคราะห์ จัดประเภท และดำเนินการแก้ไขช่องโหว่ที่พบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะดำเนินการทดสอบเจาะระบบขนาดใหญ่แบบเต็มวงจรเป็นประจำ
		8.10.5 ผู้ประกอบธุรกิจต้องนำเสนอรายงานผลการทดสอบการเจาะระบบโดยไม่ชักช้าเมื่อได้รับ การแจ้งจากสำนักงาน	และดำเนินการทดสอบเจาะระบบแบบเจาะจงอย่างยืดหยุ่นในสถานการณ์ต่างๆ เช่น ก่อนการเปิดตัวผลิตภัณฑ์ใหม่หรือเมื่อมีการเปลี่ยนแปลงครั้งสำคัญ ผลการทดสอบเจาะระบบจะแจ้งให้ฝ่ายงานผู้รับผิดชอบที่เกี่ยวข้องทราบในงานความปลอดภัย และฝ่ายงานผู้รับผิดชอบจะดำเนินการปะช่องโหว่หรือ ดำเนินการมาตรการควบคุมชนิดอื่นๆ ทันที เพื่อให้มั่นใจว่าช่องโหว่ที่ไขประโยชน์ได้ซึ่งพบในการทดสอบเจาะระบบได้รับการจัดการอย่างเหมาะสม นอกจากนี้ Tencent Cloud ยังดำเนินการฝึกซ้อมการต่อสู้เสมือนระหว่างทีมแดงและ ทีมน้ำเงินเพื่อจำลองการต้านทานการโจมตีทางเครือข่ายเป็นประจำ
			Tencent Cloud ยังได้สร้างแพลตฟอร์มรับข้อเสนอแนะช่องโหว่จากภายนอกและดำเนินการ "โครงการให้รางวัลการรายงานช่องโหว่" โดยเชิญผู้เชี่ยวชาญด้านความปลอดภัยในอุตสาหกรรมช่วย Tencent Cloud ค้นพบช่องโหว่และความเสี่ยงด้านความปลอดภัยของระบบจากมุมมองของแฮกเกอร์ เพื่อแก้ไขปัญหาด้านความปลอดภัยได้ทันห่วงที่ และบำรุงรักษาความปลอดภัยของระบบนิเวศของ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Tencent Cloud
8.11	การบริหารจัดการโปรแกรมแก้ไขช่องโหว่	โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่ในระบบและอุปกรณ์เพื่อลดความเสี่ยงที่จะถูกโจมตีในอนาคต	ลูกค้าควรกำหนดขั้นตอนการติดตั้งแพตช์ซ่อมช่องโหว่ (security patch) สำหรับระบบและอุปกรณ์ โดยดำเนินการติดตั้งแพตช์ตามระดับความรุนแรงของแพตช์และความสำคัญของระบบเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยงจากการถูกโจมตีในอนาคต ลูกค้ายังสามารถใช้ Cloud Workload Protection Platform (CWPP) เพื่อตรวจจับช่องโหว่ซอฟต์แวร์ Linux ช่องโหว่ระบบปฏิบัติการ Windows ช่องโหว่ Web-CMS และช่องโหว่แอปพลิเคชัน แจ้งเตือนแบบเรียลไทม์ และรับโซลูชันการแก้ไขช่องโหว่ ช่วยลูกค้าตอบสนองต่อความเสี่ยงจากช่องโหว่อย่างรวดเร็ว Tencent Container Security Service (TCSS) เป็นระบบแพตช์เสมือนที่ Tencent Cloud Security พัฒนาขึ้นเพื่อป้องกันช่องโหว่วันศูนย์ (zero-day) ที่เกิดขึ้นบ่อยครั้ง ซึ่งผสมผสานเทคโนโลยีการขุดเจาะช่องโหว่และการแจ้งเตือนช่องโหว่ร้ายแรงแบบเรียลไทม์ของ Tencent ใช้เพื่อตรวจจับและวิเคราะห์ช่องโหว่ สร้างแพตช์เสมือนตามความรู้ความเชี่ยวชาญของ Tencent และทำให้แพตช์เสมือนมีผลบนเซิร์ฟเวอร์คลาวด์โดยอัตโนมัติ เพื่อป้องกันการโจมตีของแฮกเกอร์ได้อย่างมีประสิทธิภาพ นอกจากนี้ ลูกค้ายังสามารถใช้ Vulnerability Scanning Service (VSS) เพื่อดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของอุปกรณ์เครือข่ายและบริการแอปพลิเคชันขององค์กร และใช้คำแนะนำการแก้ไขที่มีประสิทธิภาพจาก VSS เพื่อลดความเสี่ยงด้านความปลอดภัยขององค์กร เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านการจัดการแพตช์ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะระบุแพตช์ล่าสุด และดำเนินการทดสอบความปลอดภัยอย่างเพียงพอก่อนการติดตั้งแพตช์ เพื่อให้มั่นใจในความปลอดภัยของการติดตั้งแพตช์ Tencent Cloud จะแจ้งให้ทีมงานธุรกิจภายในแต่ละทีมทราบเป็นประจำเกี่ยวกับการอัปเดตและติดตั้งแพตช์ และใช้เครื่องมือตรวจสอบจุดปลายทาง (endpoint) สแกนสถานะการติดตั้งแพตช์เป็นประจำ และอุปกรณ์ที่ไม่ได้ติดตั้งแพตช์เกินกำหนดเวลาจะถูกสร้างใบงานแจ้งเตือนโดยอัตโนมัติ ในเวลาเดียวกัน Tencent Cloud ยังได้สร้างกลไกการสแกนช่องโหว่ภายในและแพลตฟอร์มรวบรวมช่องโหว่ภายนอก เพื่อรายงานปัญหาช่องโหว่และภัยคุกคามทั้งภายในและภายนอก ใบงานช่องโหว่ความปลอดภัยจะถูกบันทึกไว้ในระบบปฏิบัติการความปลอดภัยและถูกกำหนดให้ผู้รับผิดชอบที่เกี่ยวข้องดำเนินการภายในเวลาที่กำหนด นอกจากนี้ ทีมวิจัยความปลอดภัยของ Tencent Cloud ได้พิสูจน์ความสามารถในการป้องกันช่องโหว่ลงในระบบไฟร์วอลล์แอปพลิเคชันเว็บของ Tencent Cloud ในรูปแบบแพตช์เสมือน เพื่อให้มั่นใจในความปลอดภัยโดยรวมของแพลตฟอร์มคอมพิวเตอร์คลาวด์
9	การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร	ผู้ประกอบการธุรกิจต้องมีการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่าย สื่อสารอย่างเหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่ได้รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งพร้อมให้บริการได้อย่างต่อเนื่อง	ลูกค้าควรสร้างกลไกการป้องกันความปลอดภัยของการสื่อสารเครือข่าย เพื่อรับประกันความปลอดภัยและความเสถียรของเครือข่ายการสื่อสารและข้อมูลที่ส่ง และดำเนินการหรือติดตั้งอุปกรณ์ความปลอดภัยเครือข่ายที่จำเป็น เพื่อป้องกันภัยคุกคามและบุกรุกทางความปลอดภัยเครือข่าย Tencent Cloud มีอยู่ทั่วโลกหลายภูมิภาคทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) ครอบคลุมพื้นที่จีนแผ่นดินใหญ่ ภูมิภาคเอเชียแปซิฟิก ภูมิภาคอเมริกาเหนือ และภูมิภาคยุโรป ลูกค้าสามารถปรับใช้ข้อมูลและระบบในภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระและยืดหยุ่นตามความต้องการในการพัฒนาธุรกิจและข้อกำหนด

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ด้านความปลอดภัยของข้อมูล เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติ (disaster recovery) เครือข่ายพื้นฐานของ Tencent Cloud ใช้วิธีการก่อสร้างแบบซ้ำซ้อน ร่วมกับการจัดลำดับความสำคัญของเส้นทางในระดับการกำหนดเส้นทางและการจัดสรรการจราจรเพื่อความสามารถในการเข้าถึงเส้นทาง เพื่อให้มั่นใจว่าบริการเครือข่ายจะไม่หยุดชะงักเนื่องจากความล้มเหลวของอุปกรณ์ใดตัวเดียว โหมดการคำนวณของ Tencent Cloud ยังใช้วิธีการก่อสร้างแบบซ้ำซ้อน โดยเมื่อโหมดการคำนวณเดียวเกิดความล้มเหลวจะถูกตัดออกโดยอัตโนมัติแบบเรียลไทม์ผ่านตัวจัดการกำหนดการ ซึ่งรับประกันความพร้อมใช้งานของธุรกิจลูกค้าได้อย่างมีประสิทธิภาพ ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจว่ามีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า Direct Connect (DC): จัดเตรียมการเชื่อมต่อเครือข่ายแบนด์วิดท์สูงที่มีความเฉพาะตัวและความปลอดภัยสูง ผู้ใช้เป็นเจ้าของลิงก์เครือข่ายโดยเฉพาะ ไม่มีความเสี่ยงข้อมูลรั่วไหล นอกจากนี้ ลูกค้ายังสามารถใช้ Cloud Connect Network (CCN) เพื่อให้บรรลุการเชื่อมต่ออินทราเน็ตที่ปลอดภัยระหว่าง Virtual Private Cloud (VPC) บนคลาวด์ และระหว่าง VPC กับศูนย์ข้อมูลในพื้นที่ (IDC) สำหรับข้อกำหนดการแบ่งส่วนเครือข่าย ลูกค้าสามารถใช้บริการ Virtual Private Cloud (VPC) ที่ Tencent Cloud ให้มาเพื่อสร้างพื้นที่เครือข่ายอิสระหลายแห่งสำหรับทรัพยากรแพลตฟอร์มคลาวด์ที่ได้ซื้อไปแล้ว

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และกำหนดการแบ่งส่วนเครือข่ายและที่อยู่ IP นโยบายการกำหนดเส้นทาง ฯลฯ ตามต้องการได้ด้วยตนเอง บริการ VPC เป็นพื้นที่เครือข่ายบนคลาวด์เฉพาะที่สร้างขึ้นบน Tencent Cloud โดยเครือข่ายส่วนตัวใช้เทคโนโลยีโมิงค์ สร้างเครือข่ายเสมือนบนเครือข่ายกายภาพ และใช้เทคโนโลยีเสมือนจริง เพื่อให้บรรลุการแยกอินทราเน็ตโดยสมบูรณ์ระหว่างเครื ข่ายส่วนตัวต่างๆ มอบเครือข่ายคลาวด์ที่ปลอดภัยเป็นอิสระและแยกจาก กันให้กับลูกค้า สำหรับเซิร์ฟเวอร์คลาวด์ภายในเครือข่ายส่วนตัว สามารถควบคุมการไหลเข้าออกของข้อมูลในระดับอินส แตนซ์และซับเน็ตได้ผ่านการกำหนดค่ากลุ่มความปลอด ภัยและกฎ Access Control List (ACL) ของเครือข่าย เพื่อให้บรรลุการควบคุมการเข้าถึงเครือข่ายในระดับต่าง ๆ เพื่อดำเนินการป้องกันขอบเขตเครือข่าย Tencent Cloud ให้บริการ EdgeOne (EO) แก่ลูกค้า โดยอิงตามโหมดขอบทั่วโลกรของ Tencent Cloud เพื่อบริการป้องกันความปลอดภัยและเร่งความเร็วใ ห้กับลูกค้า มีฟังก์ชัน เช่น การป้องกัน DDoS การป้องกันเว็บอภัยริยะ การป้องกันการโจมตีประเภทบอท/ครอว์เลอร์ การแก้ไข DNS และสนับสนุนให้ลูกค้าสามารถกำหนดกฎการควบคุมก ารเข้าถึงแบบกำหนดเองตามความต้องการทางธุรกิจ Cloud Firewall (CFW) ให้การป้องกันขอบเขตเครือข่ายที่แตกต่างกันแก่ลูกค้า เป็นหลัก สนับสนุนการควบคุม ACL ของไฟร์วอลล์อย่างเข้มข้น การปิดกั้น IPS แบบเรียลไทม์ การปะชุดเสมือน และการตรวจจับโค้ดที่เป็นอันตราย ฯลฯ สามารถตอบสนองความต้องการของโซน DMZ ในเครือข่ายแบบดั้งเดิม ปกป้องสินทรัพย์หลักเป็นพิเศษ และบรรลุการควบคุมการแยกอย่างละเอียดระหว่าง VPC Web Application Firewall (WAF) สามารถจัดการกับปัญหาความปลอดภัยของเว็บไซต์แ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ละเมิดลิขสิทธิ์ เช่น การโจมตีเว็บไซต์ การบุกรุก การใช้ประโยชน์จากช่องโหว่ การฝังมัลแวร์ การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต แฮกเกอร์ ครอว์เลอร์ ฯลฯ Anti-DDoS ใช้ทรัพยากรป้องกัน DDoS ที่มีคุณภาพและเพียงพอ ร่วมกับอัลกอริทึมการทำความสะอาดที่พัฒนาอย่างต่อเนื่อง เนื่อง "การพัฒนาด้วยตนเอง + การระบุอัจฉริยะด้วย AI" เพื่อจัดการกับปัญหาการโจมตี DDoS ในด้านการจัดการควบคุมความปลอดภัยเครือข่าย Tencent Cloud ยังได้สร้างมาตรฐานการจัดการความปลอดภัยเครือข่าย และระบบป้องกันเครือข่ายแบบหลายชั้นภายในองค์กร Tencent Cloud กำหนดมาตรฐานการควบคุมและป้องกันความปลอดภัย เครือข่าย ตลอดจนบทบาทและความรับผิดชอบที่เกี่ยวข้องอย่าง ชัดเจนผ่านระบบการจัดการและขั้นตอนการทำงาน เพื่อให้มั่นใจว่ากิจกรรมที่ดำเนินการบนเครือข่ายของ Tencent Cloud ดำเนินไปอย่างปลอดภัย ในเวลาเดียวกัน Tencent Cloud ได้ปรับใช้สถาปัตยกรรมความปลอดภัยเครือข่ายที่ครบ ถ้วน โดยใช้กลไกการป้องกันหลายชั้น เช่น ไฟร์วอลล์ ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) การป้องกัน DDoS การแยกทางลอจิคัลของเครือข่าย และความปลอดภัยของแอปพลิเคชันเว็บ เพื่อตรวจจับ กรอง และบล็อกการรับส่งข้อมูลเครือข่ายที่เป็นอันตรายได้ทันที ทางที่ ปกป้องความปลอดภัยเครือข่ายของ Tencent Cloud นอกจากนี้ Tencent Cloud ใช้มาตรการต่างๆ เช่น การควบคุมสิทธิ์และการอนุมัติขั้นตอน เพื่อห้ามไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงทรัพยากร เครือข่ายภายใน ซึ่งรวมถึงเครื่องมือวิเคราะห์และตรวจสอบเครือข่าย สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความปลอดภัยในการสื่อสาร โปรดดูเนื้อหาในข้อ "5 การรักษาความมั่นคงปลอดภัยของระบบเครือข่าย ยสื่อสาร" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยี สารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ"

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ในคู่มือนี้
10.2	จัดหาระบบ IT	จัดให้มีหลักเกณฑ์ในการจัดหาระบบ IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและ ความต้องการด้านความมั่นคงปลอดภัย IT โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี รวมถึงการเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างมีนัยสำคัญ	ลูกค้าควรกำหนดเกณฑ์การเลือกผู้ให้บริการระบบเทคโนโลยีสารสนเทศและบริการ เพื่อให้แน่ใจว่าระบบที่จัดซื้อสามารถตอบสนองความต้องการทางธุรกิจและข้อกำหนดด้านความปลอดภัยข้อมูล Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ อิงตามความต้องการของลูกค้า ได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองต่อการตรวจสอบอย่างละเอียดของลูกค้า สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบอย่างละเอียด สามารถอ้างอิงเนื้อหาในภาคผนวก 3-2 " การคัดเลือกผู้ให้บริการภายนอก" ของบทที่ 6 " Tencent Cloud จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ หลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก ของ BOT อย่างไร" ได้อย่างไร" ในคู่มือนี้ Tencent Cloud ได้รับการรับรองและคุณวุฒิด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดความเป็นส่วนตัวหลายรายการผ่านการตรวจสอบหรือการประเมินโดยบุคคลที่สามที่เป็นอิสระ โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจาก " Compliance Document Download" Tencent Cloud ยังได้สร้างมาตรฐานการพัฒนาความปลอดภัยระบบสารสนเทศภายในองค์กร และมุ่งมั่นพัฒนาตามมาตรฐาน ISO/IEC 20000 การจัดการบริการเทคโนโลยีสารสนเทศ ระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001 และมาตรฐานระบบการจัดการคุณภาพ ISO/IEC 9001 เข้ากับกระบวนการวงจรชีวิตการพัฒนาความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ผลิตภัณฑ์ทั้งหมด ให้มีความสำคัญกับขั้นตอนต่างๆ เช่น ความต้องการ การออกแบบ การวิจัยและพัฒนา การทดสอบ การส่งมอบ และการดำเนินการและบำรุงรักษา พยานแนวคิดด้านความปลอดภัยข้อมูลและการปกป้องความเป็นส่วนตัวเข้าไปในแต่ละขั้นตอนของการพัฒนาผลิตภัณฑ์ เพื่อให้มั่นใจว่าผลิตภัณฑ์คลาวด์ได้รับความควบคุมด้านความปลอดภัยที่เพียงพอตลอดวงจรชีวิตของผลิตภัณฑ์
10.3	พัฒนาระบบ IT	จัดให้มีมาตรการควบคุมเกี่ยวกับการพัฒนาระบบ IT ในการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งานจริง เพื่อให้มั่นใจว่า ระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และ มีความยืดหยุ่นเพียงพอจะรองรับการดำเนินงานได้สอดคล้องกับแผนการดำเนินธุรกิจ โดยต้องดำเนินการอย่างน้อยดังนี้ (1) มีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนาดังนี้ (2) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง (3) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) (4) มีกระบวนการหรือเครื่องมือควบคุมการพัฒนาชุดคำสั่งคอมพิวเตอร์ให้มีความปลอดภัย	ลูกค้าควรสร้างกรอบการจัดการวงจรชีวิตการพัฒนาระบบ โดยรวมข้อกำหนดด้านความปลอดภัยในแต่ละขั้นตอนของวงจรชีวิตการพัฒนาระบบ ลูกค้าสามารถใช้เครื่องมือนักพัฒนา Cloud-Native Build (CNB) ที่ Tencent Cloud ให้มา CNB พยานแนวคิดการพัฒนารูปแบบคล่องตัว (Agile) อย่างลึกซึ้ง ตั้งแต่ issue การรวมค่าชอไปจนถึงชุดงาน กระบวนการพัฒนารูปแบบคล่องตัวได้รับการจัดตั้งขึ้นอย่างเป็นระเบียบ ช่วยลูกค้ายืนยันผลลัพธ์ของการเปิดตัวเวอร์ชันผลิตภัณฑ์สู่ตลาดด้วยงบประมาณที่ต่ำลงและวิธีการวนซ้ำที่เร็วขึ้น นอกจากนี้ Tencent Infrastructure Automation for Terraform เป็นความสามารถอัตโนมัติของ Tencent Cloud ในการปรับใช้ จัดทำ และจัดการทรัพยากร Tencent Cloud ภายใต้ระบบขยายปลั๊กอินของ Terraform ซึ่งเป็นเครื่องมือ Infrastructure as Code (IaC) ที่ได้รับความนิยมทั่วโลก โดยเชื่อมโยงความสามารถของเครื่องมืออัตโนมัติโครงสร้างพื้นฐานที่สมบูรณ์และครบถ้วนของ Terraform กับความสามารถบริการทรัพยากรคลาวด์ของ Tencent Cloud ทำให้ลูกค้าสามารถดำเนินการรูปแบบ DevOps และการปรับใช้หลายคลาวด์ (Multi-cloud) ได้อย่างสะดวก ในด้านการจัดการวงจรชีวิตการพัฒนาระบบความปลอดภัย Tencent Cloud ยังได้สร้างมาตรฐานการพัฒนาระบบความปลอดภัยระบบสารสนเทศภายในองค์กร และมุ่งมั่นพัฒนามาตรฐาน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		(5) มีการทดสอบระบบ T ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง ลงเพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถ ประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้ งาน	ISO/IEC 20000 การจัดการบริการเทคโนโลยีสารสนเทศ ระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001 และมาตรฐานระบบการจัดการคุณภาพ ISO/IEC 9001 เข้ากับกระบวนการวงจรชีวิตการพัฒนาความปลอดภัย ผลิตภัณฑ์ทั้งหมด ให้ความสำคัญกับขั้นตอนต่างๆ เช่น ความต้องการ การออกแบบ การวิจัยและพัฒนา การทดสอบ การส่งมอบ และการดำเนินการและบำรุงรักษา
		(6) มีมาตรการควบคุมความถูกต้องครบ ถ้วนของการแปลงข้อมูล (data conversion)	ผสานแนวคิดด้านความปลอดภัยข้อมูลและการปกป้อง ความเป็นส่วนตัวเข้าไปในแต่ละขั้นตอนของการพัฒนา ผลิตภัณฑ์
		(7) มีมาตรการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลสำคัญที่นำไป ใช้ในการทดสอบ	เพื่อให้มั่นใจว่าผลิตภัณฑ์คลาวด์ได้รับความควบคุมด้าน ความปลอดภัยที่เพียงพอตลอดวงจรชีวิตของผลิตภัณฑ์ เกณฑ์ มาตรการควบคุมความปลอดภัยที่เกี่ยวข้อง ได้แก่:
		(8) มีการทดสอบประสิทธิภาพ (performance test) ของระบบที่เกี่ยวข้องกับการให้บริการ หรือการทำธุรกรรมทางอิเล็กทรอนิกส์ เมื่อมีการพัฒนาหรือเปลี่ยนแปลงระบบ อย่างมีนัยสำคัญ เพื่อให้มั่นใจว่าระบบดังกล่าวสามารถ รองรับปริมาณการใช้งานได้สอดคล้องกับ ความต้องการทางธุรกิจ	การฝึกอบรมความปลอดภัย: ส่งเสริมจิตสำนึกการเขียนโปรแกรมที่ปลอดภัย สำหรับนักพัฒนา กำหนดให้นักพัฒนาปฏิบัติตามมาตรฐานการเข้ารหัสที่ปลอดภัยอย่างเคร่งครัด
		(9) ในกรณีที่มีการมอบหมายให้บุคคล ภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ผู้ประกอบการต้องจัดให้มีการติดตาม และควบคุมการดำเนินการให้เป็นไปตาม ข้อตกลงในการมอบหมายงาน	การวิเคราะห์ความต้องการ: สื่อสารเกี่ยวกับเนื้อหาและกระบวนการธุรกิจ และกรอบทางเทคนิค เพื่อค้นหาวิธีที่ดีที่สุดในการฝังความปลอดภัย
		(10) มีการขออนุมัติจากผู้บริหาร หรือคณะกรรมการที่ได้รับมอบหมาย จากผู้ประกอบการ ก่อนนำระบบขึ้นใช้งานจริง	- การออกแบบระบบ: สร้างแบบจำลองภัยคุกคามสำหรับการออกแบบระบบ และประเมินความปลอดภัยทางเทคนิคของสถาปัตยกรรมที่ใช้ - การพัฒนาระบบ: ในระหว่างกระบวนการพัฒนา จัดเตรียมส่วนประกอบการพัฒนาความปลอดภัย ที่ Tencent ออกแบบเองสำหรับนักพัฒนาใช้ และเขียนโค้ดตามมาตรฐานการเข้ารหัสความปลอดภัยของ Tencent Cloud - การยืนยันความปลอดภัย: ค้นพบช่องโหว่ผ่านการตรวจสอบความปลอดภัย ของโค้ด การสแกนความปลอดภัยของสินทรัพย์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			การสแกนเว็บ การประเมินความปลอดภัยด้วยมนุษย์ การทดสอบเจาะระบบ และการตรวจสอบโค้ด การเผยแพร่: ระบบจะเผยแพร่ไปยังสภาพแวดล้อมออนไลน์ได้ ก็ต่อเมื่อความเสี่ยงสูงทั้งหมดได้รับการแก้ไขแล้ว เพื่อป้องกันไม่ให้เกิดผลกระทบทำงานในสภาพแวดล้อมการผลิตโดยมีช่องโหว่ด้านความปลอดภัย ขั้นตอนการจัดการการเปลี่ยนแปลงและการเผยแพร่ของ Tencent Cloud ครอบคลุมการเปลี่ยนแปลงของแอปพลิเคชันและไฟล์คอนฟิก ระบบปฏิบัติการ และฐานข้อมูล โดยก่อนนำขึ้นระบบจริง การเปลี่ยนแปลงเหล่านี้จะต้องผ่านการทดสอบการทำงาน (Functional Test) แบบอิสระ หลังจากเผยแพร่การเปลี่ยนแปลงแล้ว ทีมปฏิบัติการของ Tencent Cloud จะทำการทดสอบย้อนกลับ (Regression Test) เพื่อตรวจสอบผลกระทบของการเปลี่ยนแปลงระบบ นอกจากนี้ Tencent Cloud ยังได้กำหนดกลไกนโยบายการให้สิทธิ์และการแยกเมทริกซ์สิทธิ์ในการควบคุมการเข้าถึงภายใน เพื่อรับรองการแยกหน้าที่ระหว่างบุคลากรที่เกี่ยวข้องกับการพัฒนาซอฟต์แวร์ การทดสอบ และการเผยแพร่ Tencent Cloud รับรองว่าสภาพแวดล้อมการพัฒนา/ทดสอบและสภาพแวดล้อมการผลิตถูกแยกออกจากกัน และห้ามใช้ข้อมูลการผลิตที่ยังไม่ได้ปิดในสภาพแวดล้อมการพัฒนา/ทดสอบ สำหรับการใช้ผลิตภัณฑ์บุคคลที่สาม Tencent Cloud ได้กำหนดข้อกำหนดด้านการจัดการความปลอดภัยของซัพพลายเชน โดยกำหนดให้ต้องมีการตรวจสอบการอนุญาตเข้าความปลอดภัยเมื่อนำเข้าองค์ประกอบภายนอก และจำเป็นต้องมีการเสริมความแข็งแกร่งด้านความปลอดภัยและการป้องกันก่อนการเปิดใช้งาน เพื่อให้มั่นใจว่าผลิตภัณฑ์ผ่านการตรวจสอบความปลอดภัยก่อนเปิดใช้งาน หลังผลิตภัณฑ์เปิดใช้งาน จะดำเนินการปฏิบัติการและบำรุงรักษาด้านความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ภัยและการตรวจสอบความปลอดภัยอย่างต่อเนื่อง เพื่อแก้ไขปัญหาด้านความปลอดภัยได้ทันเวลาที่ และผ่านการประเมินสถานการณ์การดำเนินงานด้านค ความปลอดภัยของผลิตภัณฑ์ เพื่อระบุความเสี่ยงด้านความปลอดภัยและกระตุ้นให้ซัพ พลายเออร์ปรับปรุง ตลอดจนทบทวนกลยุทธ์ความร่วมมือกับซัพพลายเออ รดังกล่าวในอนาคต นอกจากนี้ Tencent Cloud ยังได้สร้างมาตรฐานการจัดการความปลอดภัยของส่วน ประกอบโอเพนซอร์ส เพื่อให้มั่นใจว่าแหล่งที่มาของส่วนประกอบโอเพนซอร์ส ที่ทีมพัฒนานำเข้ามามีความน่าเชื่อถือ และผ่านการตรวจสอบความปลอดภัย เพื่อให้มั่นใจในความปลอดภัยและความถูกต้องตามกฎหมาย ในการใช้ส่วนประกอบโอเพนซอร์ส
10.4	แก้ไขเปลี่ยนแปลงระบบ IT	(1) มีการประเมินผลกระทบ และจัดลำดับความสำคัญของการเปลี่ นแปลง (2) มีกระบวนการขออนุมัติการเปลี่ย นแปลง (change request) โดยต้องได้รับการอนุมัติจาก หน่วยงานเจ้าของระบบ (system owner) เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงได้รับ การพิจารณาความจำเป็นอย่างเหมาะสมแล้ว (3) มีการทดสอบระบบก่อนนำไปตั้งค่า หรือนำไปติดตั้งบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจ เกิดขึ้น (4) มีกระบวนการขออนุมัติจากผู้บริหาร หรือคณะกรรมการที่ได้รับมอบหมาย จากผู้ประกอบธุรกิจ ก่อนนำระบบขึ้นใช้งานจริง (5) มีกระบวนการหรือเครื่องมือควบคุม การเปลี่ยนแปลงรุ่น (version) ของชุดคำสั่งคอมพิวเตอร์ (source code version control) และรองรับการถอยกลับสู่สภาพเดิม (fallback)	ลูกค้าควรกำหนดขั้นตอนการจัดการการเปลี่ยนแปลง โดยการเปลี่ยนแปลงทุกประเภทควรได้รับการประเมิน ทดสอบ ทบทวน และอนุมัติก่อนการดำเนินการ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำ กับดูแล Tencent Cloud ได้สร้างมาตรฐานการจัดการสำหรับการเปลี่ยนแปลงพ ลิตภัณฑ์และการกำหนดค่าที่กำหนดขั้นตอนต่างๆ ในกระบวนการเปลี่ยนแปลงและได้รับผิดชอบที่เกี่ยวข้อง อย่างชัดเจน เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการอนุมัติและทดสอบ อย่างเหมาะสมก่อนการดำเนินการ ในเวลาเดียวกัน Tencent Cloud ได้กำหนดขั้นตอนการจัดการสำหรับการเปลี่ยนแปลง ฉุกเฉิน โดยการเปลี่ยนแปลงฉุกเฉินต้องได้รับการอนุมัติที่เหมาะสม ก่อนจึงจะสามารถดำเนินการได้ การเปลี่ยนแปลงโปรแกรมทุกประเภ รวมถึงการเปลี่ยนแปลงแอปพลิเคชันและไฟล์กำหนดค า ระบบปฏิบัติการ และฐานข้อมูล ต้องได้รับการวิเคราะห์ผลกระทบทางธุรกิจก่อนการเปิด ตัว จัดทำแผนย้อนกลับสำหรับการเปลี่ยนแปลง และได้รับการอนุมัติจากผู้รับผิดชอบที่เกี่ยวข้อง ระบบเผยแพร่การเปลี่ยนแปลงของ Tencent Cloud บังคับให้การดำเนินการเปลี่ยนแปลงสามารถดำเนินการ ได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น และเก็บรักษาบันทึกที่เกี่ยวข้องกับการเปลี่ยนแปลงไว้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		(6)ปรับปรุงรายละเอียดประกอบระบบงานที่ได้มีการแก้ไขเปลี่ยนแปลงเพื่อให้เป็นปัจจุบัน	พร้อมทั้งตรวจสอบบันทึกเป็นประจำ หลังการเผยแพร่การเปลี่ยนแปลง Tencent Cloud จะตรวจสอบ ตรวจสอบ และบันทึกผลการเปลี่ยนแปลงในสภาพแวดล้อมการผลิต Tencent Cloud จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอการดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน และขอบเขตของการเปลี่ยนแปลง สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแวดล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขยาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม
11	การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT	ผู้ประกอบธุรกิจต้องมีการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างเหมาะสมและทันทางที่ ดังนี้ 11.1 จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง 11.2 กำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT 11.3 รายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงาน โดยไม่ชักช้า เมื่อทราบเหตุการณ์ดังกล่าว 11.4 วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทาง การแก้ไข และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต 11.5 บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าว เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่เกิดเหตุการณ์นั้น	ลูกค้าควรสร้างขั้นตอนและกระบวนการจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ และควรจัดทำแผนการสื่อสาร กำหนดผู้เกี่ยวข้องที่ต้องติดต่อและเนื้อหาการสื่อสารเมื่อเกิดเหตุการณ์ วิเคราะห์สาเหตุรากฐานของเหตุการณ์และดำเนินการมาตรการแก้ไข และเก็บรักษาด้านที่ที่เกี่ยวข้องไว้อย่างน้อยสองปี เพื่อให้สามารถเรียกดูและตรวจสอบได้ตลอดเวลา นอกจากนี้ ลูกค้ายังควรดำเนินการฝึกซ้อมเหตุการณ์ความปลอดภัยทางไซเบอร์อย่างน้อยปีละหนึ่งครั้ง และรายงานผลการตรวจสอบต่อฝ่ายบริหาร เพื่อสนับสนุนลูกค้าในการตรวจจับและตอบสนองต่อบัณฑิตเหตุอย่างรวดเร็ว Tencent Cloud ให้บริการแพลตฟอร์มการจัดการความปลอดภัยแบบครบวงจร Cloud Security Center (CSC) ผ่านฟังก์ชันต่างๆ เช่น ศูนย์สินทรัพย์ ศูนย์ความเสี่ยง ศูนย์แจ้งเตือน และการจัดการความปลอดภัยขั้นสูง ช่วยลูกค้าบรรลุวงจรการดำเนินงานความปลอดภัยได้แก่ การตรวจจับภัยคุกคามก่อนเกิดเหตุ การตอบสนองและจัดการระหว่างเกิดเหตุ และการวิเคราะห์ย้อนหลังหลังเหตุการณ์ เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้ สำนักงานสามารถเรียกดูและตรวจสอบ ได้โดยไม่ชักช้า 11.6 ทดสอบและทบทวนขั้นตอนปฏิบัติ หรือแผนการบริหารจัดการเหตุการณ์ ผิดปกติด้าน IT อย่างน้อย ปีละ 1 ครั้ง จะต้องครอบคลุมถึงการทดสอบการ บริหารจัดการเหตุการณ์ด้านภัยคุกคาม ทางไซเบอร์ (cyber security drill) และจัดให้มีการรายงานผลการทดสอบ และทบทวนต่อคณะกรรมการของผู้ปร ะกอบธุรกิจหรือคณะกรรมการ ที่ได้รับมอบหมายจากคณะกรรมการของ ผู้ประกอบการธุรกิจ	ย ในด้านการตรวจจับและตอบสนองต่อเหตุการณ์ Tencent Cloud ได้สร้างขั้นตอนการจัดการเหตุการณ์โดยละเอียด โดยใช้ระบบการดำเนินงานความปลอดภัยภายในเพื่อบ ันทึกเหตุการณ์ความปลอดภัย สำหรับเหตุการณ์ความปลอดภัยที่ตรวจจับและระบุได้ Tencent Cloud จะวิเคราะห์และจำแนกระดับเหตุการณ์โดยพิจารณาจาก ปัจจัยต่างๆ เช่น ลักษณะของเหตุการณ์ ระดับความอ่อนไหวของข้อมูล และขอบเขตของผลกระทบ และจะแจ้งให้ผู้รับผิดชอบที่เกี่ยวข้องทราบทันทีเพื่อดา เนินการจัดการเหตุการณ์ ทีมงานความปลอดภัยของ Tencent Cloud ใช้ระบบการดำเนินงานความปลอดภัยแบบ 24 ชั่วโมงทุกวัน โดยมุ่งเน้นไปที่สถานการณ์หลัก เช่น การเฝ้าระวังช่องโหว่ การติดตามแหล่งที่มาของการบุกรุก และการปิดกั้นการโจมตี ตอบสนองต่อการแจ้งเตือนความปลอดภัยแบบเรียลไทม์ และจัดทำแผนการติดตามแหล่งที่มาของการโจมตีแล ะการจัดการเหตุการณ์ฉุกเฉินอย่างรวดเร็ว เพื่อยับยั้งการแพร่กระจายของเหตุการณ์ความปลอดภัย ได้อย่างมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบ ต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัย ข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียใ ห้เหลือน้อยที่สุด ในด้านการที่ลูกค้าแจ้งปัญหาหรือติดต่อ Tencent Cloud คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการในงาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ความพร้อมใช้งาน และการรักษาความลับ ระบบในของ Tencent Cloud จะจัดลำดับความสำคัญให้กับในของลูกค้าผ่านกลไก การตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมแล ะจัดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้า ได้รับการตอบสนองและจัดการอย่างทันท่วงที นอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเ ป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พ บบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้า ได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเว ลา ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับกา รสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า ในด้านการสรุปเหตุการณ์และการปรับปรุงอย่าง ต่อเนื่อง Tencent Cloud ได้สร้างกลไกการวิเคราะห์เหตุการณ์เป็นระยะ โดยจะวิเคราะห์เหตุการณ์หลายมิติเป็นประจำ (ประเภทเหตุการณ์ ความถี่ในการเกิด ขอบเขตผลกระทบ และระดับความรุนแรง) และดำเนินการมาตรการป้องกันตามการทบทวนเหตุการณ์ และการวิเคราะห์สาเหตุรากฐาน เพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่คล้ายคลึงกันเกิดขึ้นอีก สำหรับเหตุการณ์ความปลอดภัยที่สำคัญ Tencent Cloud จะจัดตั้งทีมเฉพาะกิจเพื่อจัดทำรายงานการวิเคราะห์เ พาะเรื่องเสนอต่อฝ่ายบริหาร ในการดำเนินการฝึกซ้อมการรับมือเหตุการณ์ ทางความปลอดภัยทางไซเบอร์ หน่วยงานที่เกี่ยวข้องกับธุรกิจภายใน Tencent

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Cloud จะจัดฝึกอบรมและฝึกซ้อมแผนฉุกเฉินสำหรับเหตุการณ์ความปลอดภัยตามสถานการณ์เป็นประจำ และยังจัดฝึกอบรมทางเทคนิคให้กับพนักงานของทีมงานความปลอดภัยตามการพัฒนาของเทคโนโลยีความปลอดภัยและสถานการณ์ เพื่อให้มั่นใจว่าพนักงานเข้าใจและปฏิบัติตามข้อกำหนดและขั้นตอนการดำเนินงานด้านความปลอดภัยสูงสุด เรียนรู้มาตรฐานและแนวปฏิบัติที่ดีที่สุดด้านความปลอดภัยข้อมูลล่าสุด และสามารถตอบสนองต่อเหตุการณ์ความปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพ
12	แผนฉุกเฉินด้าน IT	ผู้ประกอบการต้องจัดให้มีแผนฉุกเฉินด้าน IT เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ซึ่งส่งผลกระทบต่อไม่สามารถให้บริการได้ตามปกติหรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่องโดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ ดังนี้ 12.1 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT 12.2 กระบวนการจัดทำแผนฉุกเฉินด้าน IT ต้องครอบคลุมการดำเนินการ 12.3 จัดให้มีระบบ IT สำรองและทรัพยากรที่จำเป็นเพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมาย ที่กำหนดไว้ 12.4 สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม 12.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อคณะกรรมการของผู้ประกอบการหรือคณะกรรมการที่	ลูกค้าควรสร้างกลไกการจัดการความต่อเนื่องของธุรกิจ จัดทำแผนความต่อเนื่องของธุรกิจที่ครอบคลุมบริการภายนอก ดำเนินการวิเคราะห์ผลกระทบทางธุรกิจ กำหนดเป้าหมายเวลาในการกู้คืน (RTO) และเป้าหมายจุดข้อมูลในการกู้คืน (RPO) ของแต่ละธุรกิจให้ชัดเจน จัดทำแผนฉุกเฉินเพื่อความต่อเนื่องของธุรกิจ และสื่อสารไปยังผู้ที่เกี่ยวข้อง นอกจากนี้ ลูกค้ายังควรตรวจสอบและทดสอบการดำเนินการตามแผนฉุกเฉินอย่างน้อยปีละครั้ง และควรสร้างและบำรุงรักษาข้อมูลการติดต่อของบุคลากรภายในและภายนอกที่เกี่ยวข้องกับเหตุการณ์ผิดปกติ เพื่อให้มั่นใจในความพร้อมใช้งานอย่างต่อเนื่องของธุรกิจลูกค้า Tencent Cloud ได้ออกแบบและนำกรอบการจัดการความต่อเนื่องของธุรกิจที่เหมาะสมกับสภาพแวดล้อมคอมพิวเตอร์คลาวด์ของตนเองไปใช้ และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจ Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภัณฑ์และบริการคลาวด์ กำหนด RTO และ RPO ของแต่ละธุรกิจให้ชัดเจน และจัดทำกลยุทธ์การตอบสนองและแผนความต่อเนื่องของธุรกิจที่แตกต่างกันตามผลการวิเคราะห์ผลกระทบทางธุรกิจ รวมถึงจัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ได้รับมอบหมายจากคณะกรรมการของ ผู้ประกอบธุรกิจ	ดยละเอียดสำหรับผลิตภัณฑ์คลาวด์
		12.6 กำหนดกระบวนการดำเนินงาน เพื่อรับมือเหตุการณ์การใช้ทรัพยากร ด้าน IT หรือการใช้ประสิทธิภาพ ของระบบงานเกินขีดจำกัดของตัวชี้วัด ที่กำหนดไว้ เช่น การจำกัดการให้บริการบางช่องทาง หรือตัดการเชื่อมต่อกับ ผู้ให้บริการหรือบุคคลภายนอกที่มีผล กระทบต่อระบบ IT เป็นต้น	ในด้านการสนับสนุนบุคลากร Tencent Cloud ได้กำหนดบทบาทของบุคลากรในกระบวนการกู้คืนธุรกิจ และกำหนดหน้าที่และความรับผิดชอบในการแบ่งงานกัน ในกระบวนการกู้คืนให้ชัดเจน สำหรับทักษะหรือตำแหน่งงานที่สำคัญ ใช้กลไกเสริม A/B Role และดำเนินการฝึกอบรมซ้อมแผนฉุกเฉินเป็นประจำ เพื่อรับประกันการดำเนินการขั้นตอนการกู้คืนที่รวดเร็ว และมีประสิทธิภาพ
		12.7 จัดให้มีรายละเอียดในการติดต่อ งานนี้เพื่อให้สามารถประสานงานในการ รายงานเหตุการณ์ผิดปกติ ด้าน IT หรือขอความช่วยเหลือจากหน่วยงาน ภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ	ร่วมกับลูกค้าในการบรรลุการกู้คืนทันเวลาที่ในสถานการณ์ที่ธุรกิจขัดข้อง ในด้านการฝึกซ้อมความต่อเนื่องของธุรกิจและการกู้คืนจากภัยพิบัติ Tencent Cloud จัดทำแผนการฝึกซ้อมโดยอิงตามแผนความต่อเนื่องของ ธุรกิจ และดำเนินการประเมินความเสี่ยงในการฝึกซ้อม พร้อมกำหนดมาตรการรับประกันที่สอดคล้องกัน เพื่อหลีกเลี่ยงผลกระทบเชิงลบต่อบริการจากการฝึกซ้อม การฝึกซ้อมการกู้คืนจากภัยพิบัติของ Tencent Cloud มักดำเนินการโดยจำลองสถานการณ์การกู้คืนจากภัย พิบัติแบบคลาสสิกที่สมจริง รวมถึงการต่อสู้ป้องกันภัยโจมตีและความล้มเหลวขนาดใหญ่ เพื่อตรวจสอบความสามารถในการกู้คืนจากภัยพิบัติของ องระบบ ความเร็วในการตอบสนอง และความสามารถในการกู้คืนอย่างครอบคลุม สำหรับปัญหาที่ค้นพบระหว่างการฝึกซ้อม Tencent Cloud จะดำเนินการแก้ไขตามมาตรการปรับปรุงที่ระบุไว้ในรายงานสรุปการฝึกซ้อม และแก้ไขแผนฉุกเฉินที่เกี่ยวข้องทันที โดยฝ่ายตรวจสอบจะกำกับดูแลและตรวจสอบสถานการณ์การแก้ไข เพื่อช่วยลูกค้าสร้างศูนย์ข้อมูลสำรอง ศูนย์ข้อมูลของ Tencent Cloud มีอยู่ทั่วโลกหลายภูมิภาค ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) ครอบคลุมพื้นที่เงินแผ่นดินใหญ่ ภูมิภาคเอเชียแปซิฟิก ภูมิภาคอเมริกาเหนือ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และภูมิภาคยุโรป ลูกค้าสามารถปรับใช้ข้อมูลและระบบในภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระและยืดหยุ่นตามความต้องการในการพัฒนาธุรกิจและข้อกำหนดด้านความปลอดภัยของข้อมูล เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติ (disaster recovery) ของธุรกิจ จุดทางออกเครือข่ายของแต่ละโซนความพร้อมใช้งานเชื่อมต่อกับผู้ให้บริการหลายราย เพื่อสร้างความสามารถในการกู้คืนจากภัยพิบัติข้ามภูมิภาคของเครือข่าย Tencent Cloud และลดผลกระทบที่ต่อเนื่องจากการขัดข้องของเครือข่ายสาธารณะของผู้ให้บริการอย่างมีประสิทธิภาพ เครือข่ายพื้นฐานของ Tencent Cloud ใช้วิธีการก่อสร้างแบบซ้ำซ้อน ร่วมกับการจัดลำดับความสำคัญของเส้นทางในระดับการกำหนดเส้นทางและการจัดสรรการจราจรเพื่อความสามารถในการเข้าถึงเส้นทาง เพื่อให้มั่นใจว่าบริการเครือข่ายจะไม่หยุดชะงักเนื่องจากความล้มเหลวของอุปกรณ์จุดเดียว โหมดการคำนวณของ Tencent Cloud ยังใช้วิธีการก่อสร้างแบบซ้ำซ้อน โดยเมื่อโหมดการคำนวณเดียวเกิดความล้มเหลวจะถูกตัดออกโดยอัตโนมัติแบบเรียลไทม์ผ่านตัวจัดกำหนดการ ซึ่งรับประกันความพร้อมใช้งานของธุรกิจลูกค้าได้อย่างมีประสิทธิภาพ

11.4 ภาคผนวก 4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
2	การวางแผนและกำหนด ขอบเขตการ ตรวจสอบ	ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงด้าน IT และ ประกาศที่ สร. 38/2565 โดยต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวน	ลูกค้าควรให้มั่นใจว่ามีการทบทวนแผนและขอบเขตการตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง เพื่อให้แน่ใจว่าแผนและขอบเขตการตรวจสอบสอดคล้องกับประกาศที่ 38/2565 เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		กล่าว	ชุดแล Tencent Cloud ได้สร้างขั้นตอนการจัดการการตรวจสอบ กำหนดวิธีการดำเนินการตรวจสอบภายในสำหรับระบบก การจัดการความปลอดภัยข้อมูลของ Tencent Cloud อย่างชัดเจน เพื่อให้มั่นใจว่าการตรวจสอบภายในจะดำเนินการอย่างมีป ระสิทธิภาพเป็นประจำ กระบวนการตรวจสอบรวมถึงการจัดทำแผนการตรวจสอบ บ การกำหนดผู้ตรวจสอบภายใน การดำเนินการตรวจสอบภายใน และการดำเนินมาตรการแก้ไขและการตรวจสอบติดตาม ผล นอกจากนี้ Tencent Cloud ยังได้รับใบรับรองและคุณวุฒิด้านความปลอดภัยและการป ฏิบัติตามข้อกำหนดความเป็นส่วนตัวหลายรายการ เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, SOC ซึ่งพิสูจน์ว่าการจัดการความปลอดภัยและการสร้างการป องกันข้อมูลส่วนบุคคลของ Tencent Cloud เป็นไปตามมาตรฐานการรับรองที่เกี่ยวข้องหรือแนวปฏิบัติ ที่ดีของอุตสาหกรรม และยังได้รับการตรวจสอบจากสถาบันตรวจสอบบุคคลที่ส วามมีอาชีพเป็นประจำอีกด้วย
3	ดำเนินการตร วสอบเทคโนโลยีสารสนเทศ	การตรวจสอบด้าน IT ตาม แผนงานและขอบเขตที่กำหนด : 3.1 จัดให้มีการตรวจสอบและรายงาน ผลการตรวจสอบด้าน IT 3.2 จัดให้มีการบันทึกข้อมูลเกี่ยวกับ การตรวจสอบ เช่น กระดาษทำการ (working paper) และหลักฐานประกอบการตรวจเป็น ต้น เป็นระยะเวลาไม่น้อยกว่า 2 ปีนับแต่วันที่จัดทำรายงานและแผน ดังกล่าวโดยต้องจัดเก็บไว้ในลักษณะ ที่พร้อมให้สำนักงานสามารถเรียกดู และตรวจสอบได้โดยไม่ชักช้า	ลูกค้าควรดำเนินการตรวจสอบอย่างครอบคลุมตามแผน และขอบเขตการตรวจสอบเป็นประจำ จัดทำรายงานการตรวจสอบและเสนอต่อฝ่ายบริหาร และหลังจากได้รับอนุมัติแล้ว ให้ส่งต่อหน่วยงานกำกับดูแลตามวิธีที่หน่วยงานกำกับดูแล กำหนด เก็บรักษาบันทึกที่เกี่ยวข้องกับการตรวจสอบไว้อย่างน้อย สองปี เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ชุดแล Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์จ ริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud
5	การจัดทำและ รายงานผล การตรวจสอบ	5.1 เสนอรายงานผลการตรวจสอบต ามข้อ 3. ละแผนการปรับปรุงแก้ไขข้อบกพร ่องต่อคณะกรรมการของผู้ประกอบธุรกิจ	จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเท ศไทย ทีมงานด้านความปลอดภัยของ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		กิจกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือ คณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็น สาขาของธนาคารพาณิชย์ต่างประเทศ โดยไม่ซ้ำซ้อน 5.2 รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณา จากคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือ คณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็น สาขาของธนาคารพาณิชย์ต่างประเทศ ตามข้อ 5.1 ต่อสำนักงาน ตามรูปแบบและวิธีการ ที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายใน 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่ดำเนินการตรวจสอบตามข้อ 3. เว้นแต่ในกรณีที่ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่มี หน้าที่ต้องรายงานผลการตรวจสอบตามประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 19/2561 เรื่อง หลักเกณฑ์เงื่อนไขและวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ 3 กรกฎาคม พ.ศ. 2561 ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลปฏิบัติตาม ประกาศดังกล่าว 5.3 จัดเก็บรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องเป็นระยะเวลา ไม่น้อยกว่า 2 ปี นับแต่วันที่ทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะ	จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบการจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็นอิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจาก " Compliance Document Download"

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ที่พร้อมให้สำนักงานสามารถเรียกดู และตรวจสอบได้โดยไม่ชักช้า	
4	การจัดให้มีแผน การปรับปรุง แก้ไขข้อบกพร่องจาก การตรวจสอบ ด้าน IT และ การติดตามค วามคืบหน้า	จัดให้มีแผนการปรับปรุงแก้ไขข้อบกพร่องจากการตรวจสอบด้าน IT ตามข้อ 3. ที่เหมาะสมกับความเสี่ยงจากข้อบกพร่อง และติดตามความคืบหน้าในการดำเนินการ ตามแผนดังกล่าว	ลูกค้าควรจัดทำแผนแก้ไขที่สอดคล้องกันสำหรับข้อบกพร่องด้านความเสี่ยงที่พบในการตรวจสอบเทคโนโลยีสารสนเทศ และติดตามการดำเนินการตามมาตรการแก้ไข ในระหว่างกระบวนการตรวจสอบ Tencent Cloud จะจัดเตรียมหลักฐานเกี่ยวกับการออกแบบและ/หรือประสิทธิภาพในการดำเนินงานของกิจกรรมควบคุมที่เกี่ยวข้องกับเป้าหมายการควบคุม ตามข้อกำหนดของสถาบันตรวจสอบ สำหรับปัญหาที่พบในการตรวจสอบ Tencent Cloud จะวิเคราะห์สาเหตุรากฐานของปัญหาอย่างลึกซึ้ง และจัดทำและดำเนินมาตรการแก้ไขและแผนการแก้ไขที่สอดคล้องกันตามนั้น หากปัญหาที่เกี่ยวข้องอาจส่งผลกระทบต่อการใช้งานทางธุรกิจหรือความปลอดภัยของข้อมูลของลูกค้าสถาบันการเงิน Tencent Cloud จะแจ้งให้สถาบันการเงินที่เกี่ยวข้องทราบทันที Tencent Cloud จะติดตามการดำเนินการตามมาตรการแก้ไขและแผนการแก้ไขเป็นประจำ จนกว่าการตรวจสอบพบจะถูกปิด

12

Tencent Cloud จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ SEC Cloud Computing Practice อย่างไร

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (SEC) ได้จัดทำ [Cloud Computing Practice](#) ขึ้นโดยพิจารณาจากความต้องการของผู้ประกอบธุรกิจบริการหลักทรัพย์ และอิงตามกรอบมาตรฐานการจัดการระดับสากล

แนวทางนี้ครอบคลุมกระบวนการจัดการที่สำคัญในการใช้งานคอมพิวเตอร์คลาวด์ โดยมีวัตถุประสงค์เพื่อให้แนวทางการจัดการความปลอดภัยแก่หน่วยงานปฏิบัติงาน

ข้อกำหนดหลักครอบคลุมการเลือกและการประเมินผู้ให้บริการคลาวด์ สัญญาและข้อตกลงบริการ การดำเนินงานคอมพิวเตอร์คลาวด์ การตรวจสอบและประเมินผู้ให้บริการ รวมถึงการยุติและเลิกใช้บริการ

ในบทนี้ Tencent Cloud จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จาก Cloud Computing Practice และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud จะช่วยผู้ประกอบธุรกิจบริการหลักทรัพย์ในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
2.2.1	การประเมินและคัดเลือกผู้ให้บริการ	- ประกอบธุรกิจควรกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกผู้ให้บริการ Cloud Computing ที่ชัดเจน และ - มีการตรวจสอบความพร้อมและพิจารณาความเหมาะสมของผู้ให้บริการเพื่อให้มั่นใจว่าผู้ให้บริการสามารถให้บริการได้อย่างต่อเนื่อง โดยคำนึงถึงปัจจัยสำคัญ ได้แก่ ความรู้ความสามารถ ประสบการณ์ ความสามารถทางการเงินที่สามารถให้การให้บริการอย่างต่อเนื่อง	ลูกค้าควรกำหนดขั้นตอนหรือมาตรฐานในการเลือกผู้ให้บริการคอมพิวเตอร์คลาวด์ และดำเนินการตรวจสอบอย่างละเอียด (due diligence) ต่อผู้ให้บริการ เพื่อให้มั่นใจว่าผู้ให้บริการมีความสามารถในการให้บริการอย่างต่อเนื่อง การตรวจสอบควรพิจารณาประเด็นหลักๆ เช่น ความสามารถทางวิชาชีพ ความสามารถทางเทคนิค ประสบการณ์การดำเนินงาน ความสามารถทางการเงิน สถานะการรับรองความปลอดภัยเทคโนโลยีสารสนเทศ การตรวจสอบโดยอิสระ และความต่อเนื่องทางธุรกิจของผู้ให้บริการ Tencent Cloud
		- ประเมินมาตรฐานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ ได้แก่ การรักษาความลับข้อมูล (Confidentiality) ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ (Integrity) และความต่อเนื่องของการให้บริการ (Availability) เช่น ผลการประเมินมาตรฐานความปลอดภัยที่เป็นที่ยอมรับในสากล ได้แก่ ISO27001, ISO27017, PCI/DSS, TIA เป็นต้น - ประเมินผลรายงานการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ - ด้านมาตรฐานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น System and Organisation Control (SOC) Report	ได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบอย่างละเอียดของลูกค้าอย่างแข็งขัน ต่อไปนี้เป็นภาพรวมของ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ในด้านต่างๆ ของการตรวจสอบอย่างละเอียด: ความสามารถทางวิชาชีพและทางเทคนิค: Tencent Cloud ได้แสดงความสามารถทางเทคนิคที่ครอบคลุมในฐานะผู้นำในอุตสาหกรรมผ่านเทคโนโลยีคอมพิวเตอร์คลาวด์ที่แข็งแกร่ง - ความสามารถในการประมวลผลข้อมูลขนาดใหญ่ - การประยุกต์ใช้ปัญญาประดิษฐ์ - การป้องกันความปลอดภัยทางไซเบอร์ - เทคโนโลยีคลาวด์เนทีฟ - การกระจายตัวของศูนย์ข้อมูลทั่วโลก - และโซลูชันอุตสาหกรรม ความสามารถทางเทคนิคเหล่านี้ไม่เพียงรับประกันความมั่นคงและความน่าเชื่อถือของบริการ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		โดยพิจารณาถึงขอบเขตการตรวจสอบ ระยะเวลาที่ครอบคลุมในรายงานการตรวจสอบ ผลการตรวจสอบและประเด็นสำคัญในผลการตรวจสอบ ความสามารถและความน่าเชื่อถือของผู้ตรวจสอบ เป็นต้น ทั้งนี้ผู้ประกอบธุรกิจควรพิจารณาถึงรายละเอียดประกอบในรายงานการตรวจสอบ • ประเมินความสอดคล้องกันของแนวทางการรักษาความต่อเนื่องของกาให้บริการของผู้ให้บริการระบบ Cloud Computing และผลการประเมินผลกระทบทางธุรกิจ (Business Impact Analysis) ของระบบงานที่มีการใช้การบริการระบบ Cloud Computing อันประกอบไปด้วย ระยะเวลาการหยุดชะงักของระบบให้ บริการที่ยอมรับได้ (Maximum Tolerable Downtime: MTD) ระยะเวลาที่ยอมรับได้ในการกู้คืนระบบงานและข้อมูล (Recovery Time Objective: RTO) และชุดข้อมูลล่าสุดที่จะกู้คืนได้ (Recovery Point Objective: RPO) • ประเมินความเสี่ยงและแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และความต่อเนื่องในการให้บริการในกรณีที่ผลการประเมินผู้ให้บริการไม่เป็นไปตามข้อกำหนดหรือมาตรฐานความปลอดภัยที่กำหนดไว้	เท่านั้น แต่ยังจัดเตรียมสภาพแวดล้อมคอมพิวเตอร์คลาวด์ที่ปลอดภัยและน่าเชื่อถือให้กับลูกค้าด้วย ความสามารถด้านความปลอดภัยในการดำเนินงานที่ครบถ้วนของ Tencent Cloud ยังสามารถให้การสนับสนุนทางเทคนิครอบนาฬิกาสำหรับผลิตภัณฑ์คลาวด์แก่ลูกค้าได้ • ประสบการณ์ในการดำเนินงาน: ความสามารถในการดำเนินงานและขนาดของ Tencent Cloud อยู่ในตำแหน่งผู้นำในอุตสาหกรรม ศูนย์ข้อมูลของ Tencent Cloud มีการกระจายตัวอยู่ในหลายภูมิภาคทั่วโลก ครอบคลุมพื้นที่จีนแผ่นดินใหญ่ ภูมิภาคเอเชียแปซิฟิก ภูมิภาคอเมริกาเหนือ และภูมิภาคยุโรป • สภาพทางการเงิน: Tencent Cloud ซึ่งเป็นแบรนด์คอมพิวเตอร์คลาวด์ที่ Tencent Group สร้างขึ้นด้วยความอุตสาหกรรม ได้รับประโยชน์จากความแข็งแกร่งทางการเงินและสภาพทางการเงินที่มั่นคงของ Tencent Group นับตั้งแต่ปี 2010 ที่ Tencent Cloud เริ่มให้บริการคลาวด์แก่สาธารณะอย่างเป็นทางการ Tencent Cloud ได้บรรลุแนวโน้มการเติบโตที่โดดเด่นในตัวชี้วัดทางการเงินที่สำคัญ เช่น รายได้และผลกำไร Tencent Cloud ได้รับการยอมรับจากสถาบันวิจัยอุตสาหกรรมระดับโลกชั้นนำ Gartner ติดต่อกันเป็นเวลาสี่ปี โดยอยู่ในอันดับที่สองในด้านมิติด้านกลยุทธ์ในหมวดผู้ผลิตจากประเทศจีน • มาตรฐานความปลอดภัยเทคโนโลยีสารสนเทศ: เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูล ซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยข้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดการความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ รวมถึงขึ้นการทำงานประจำวันและกระบวนการจัดการของหน่วยงานและพนักงานทุกหน่วยในบริษัท นโยบายความปลอดภัยข้อมูลของ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัยบนคลาวด์สอดคล้องกับนโยบายความปลอดภัยมาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบายความปลอดภัยข้อมูล พนักงานสามารถดูนโยบายเหล่านี้ที่ Tencent Cloud เผยแพร่ผ่านแพลตฟอร์มภายในได้ นอกจากนี้ Tencent Cloud ยังได้รับใบรับรองและคุณวุฒิด้านความปลอดภัยและการปฏิบัติตามข้อกำหนดเป็นส่วนตัวหลายรายการ เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, SOC ซึ่งพิสูจน์ว่าการจัดการความปลอดภัยและการสร้างการป้องกันข้อมูลส่วนบุคคลของ Tencent Cloud เป็นไปตามมาตรฐานการรับรองที่เกี่ยวข้องหรือแนวปฏิบัติที่ดีของอุตสาหกรรม และยังได้รับการตรวจสอบจากสถาบันตรวจสอบบุคคลที่สามมืออาชีพเป็นประจำอีกด้วย การตรวจสอบโดยอิสระ: Tencent Cloud ยังได้รับการตรวจสอบโดยบุคคลที่สามมืออาชีพเป็นประจำ โดยผ่านการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายการล่าสุดได้ด้วยตนเองจาก "Compliance Document Download" ความต่อเนื่องทางธุรกิจ: Tencent Cloud ได้รับการรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจแล้ว Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภัณฑ์และบริการคลาวด์ และจัดทำกลยุทธ์การตอบสนองที่แตกต่างกัน แผนความต่อเนื่องของธุรกิจ และแผนการกู้คืนจากภัยพิบัติตามผลการวิเคราะห์ เพื่อขึ้นข้อควรระวังในการกู้คืนทรัพยากรทางธุรกิจที่เกี่ยวข้อง ของ Tencent Cloud ได้จัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดยละเอียดสำหรับผลิตภัณฑ์คลาวด์ และดำเนินการฝึกซ้อมตามแผนกู้คืนจากภัยพิบัตินั้นอย่างเคร่งครัดตามข้อกำหนดเป็นประจำ เพื่อรับประกันความทันเวลาความเป็นไปได้ของแผนกู้คืนจากภัยพิบัติ
2.2.2	การทำสัญญา และข้อตกลง การให้บริการ	• ในการจัดทำสัญญาและข้อตกลงการให้บริการ ผู้ประกอบธุรกิจต้องจัดให้มีเงื่อนไขและมาตรการเพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศในการใช้งานระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตาม ความต้องการของผู้ใช้งาน ที่ครอบคลุมเงื่อนไขสำคัญอย่างน้อยดังนี้ ก. อดทนร่วมกันระหว่างผู้ให้บริการและผู้ให้บริการซึ่งมีรายละเอียด ข. คุณสมบัติด้านความปลอดภัยของผู้ให้บริการรายอื่นที่รับดำเนินการซึ่งเทียบเท่ากับผู้ให้บริการหรือเป็นไปตาม มาตรฐานสากล ค. การติดตาม ประเมินและทบทวนการให้บริการของผู้ให้บริการ ง. ขั้นตอนการโอนย้ายข้อมูลไปยังผู้ให้บริการรายใหม่ในกรณีที่มีการเปลี่ยนตัวผู้ให้บริการ • ผู้ประกอบธุรกิจควรจัดทำสัญญาการใช้บริการจากผู้ให้บริการ อย่างเป็นลายลักษณ์อักษร และมีการจัดทำข้อตกลงการ	ลูกค้าควรทำข้อตกลงบริการ สัญญา ข้อตกลงระดับการให้บริการ (SLA) และเอกสารกฎหมายอื่นๆ กับผู้ให้บริการ ซึ่งอย่างน้อยควรครอบคลุมถึงความรับผิดชอบและหน้าที่ของทั้งสองฝ่าย ข้อกำหนดด้านความปลอดภัย การรักษาความลับของข้อมูล สิทธิในการตรวจสอบ และการจัดการผู้รับช่วงงาน นอกจากนี้ ลูกค้าควรเผื่อไว้และทบทวนบริการของผู้ให้บริการเป็นประจำ และควรกำหนดขั้นตอนการย้ายข้อมูลเมื่อเปลี่ยนผู้ให้บริการให้ชัดเจน Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสองฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ให้บริการ (Service Level Agreement) อย่างชัดเจนครอบคลุม ประเด็นที่เกี่ยวข้องดังต่อไปนี้	
2.2.3	การจัดโครงสร้างองค์กร	ให้บริการ (Service Level Agreement) อย่างชัดเจนครอบคลุม ประเด็นที่เกี่ยวข้องดังต่อไปนี้ • มีการกำหนดบทบาทหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ประกอบธุรกิจและผู้ให้บริการอย่างชัดเจน • มีการกำหนดช่องทางติดต่อและผู้รับผิดชอบด้านปัญหาการใช้งานและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ • มีการจัดทำรายชื่อหน่วยงานที่เกี่ยวข้องในการกำกับดูแล (Authorities) และช่องทางติดต่อทั้งในส่วนของผู้ประกอบธุรกิจและผู้ให้บริการครอบคลุมถึงหน่วยงานทั้งภายในประเทศและต่างประเทศที่มีการจัดเก็บข้อมูลและประมวลผลโดยผู้ให้บริการ	ลูกค้าควรกำหนดหน้าที่และความรับผิดชอบด้านความปลอดภัยระหว่างตนกับผู้ให้บริการให้ชัดเจน และกำหนดให้ผู้ให้บริการแต่งตั้งผู้ประสานงานเฉพาะเพื่อรับผิดชอบในการจัดการปัญหาเกี่ยวกับการใช้งานและความปลอดภัยระหว่างการให้บริการ นอกจากนี้ ลูกค้ายังควรจัดทำรายชื่อผู้ประสานงานกับหน่วยงานกำกับดูแลที่เกี่ยวข้อง Tencent Cloud ยึดถือคุณลักษณะของความเปิดกว้างและการแบ่งปันของบริการคอมพิวเตอร์คลาวด์ เพิ่มความสามารถด้านความปลอดภัยของแพลตฟอร์มคลาวด์และบริการคลาวด์อย่างต่อเนื่อง และร่วมกับลูกค้าสร้างระบบการรับประกันความปลอดภัยที่ดีขึ้นและสมบูรณ์ยิ่งขึ้นสำหรับธุรกิจและข้อมูลบนคลาวด์ ในฐานะผู้ให้บริการคลาวด์ Tencent Cloud รับผิดชอบด้านโครงสร้างพื้นฐานของศูนย์ข้อมูลและความปลอดภัยของแพลตฟอร์มคลาวด์ โดยคำนึงถึงว่าเมื่อลูกค้าเลือกประเภทบริการคลาวด์ที่แตกต่างกัน (เช่น บริการ IaaS, PaaS และ SaaS) สิทธิในการควบคุมส่วนประกอบต่างๆ จะแตกต่างกันไป ดังนั้น Tencent Cloud จึงสร้างโมเดลการแบ่งปันความรับผิดชอบด้านความปลอดภัยบนคลาวด์ตามประเภทบริการคลาวด์ที่แตกต่างกัน รายละเอียดสามารถอ้างอิงได้จากบทที่ 3 "โมเดลการแบ่งปันความรับผิดชอบด้านความปลอดภัยของ Tencent Cloud" ในคู่มือนี้ ตามเป้าหมายและโมเดลการแบ่งปันความรับผิดชอบดังกล่าว Tencent Cloud จะร่วมมือกับลูกค้าในการรับมือกับปัญหาด้านความปลอดภัยและความท้าทายทุกประเภทอย่างลึกซึ้งยิ่งขึ้น นอกจากนี้ Tencent Cloud ได้รวบรวมทีมบริการผู้เชี่ยวชาญที่เชี่ยวชาญในอุตสาหกรรม มุ่งมั่นให้บริการผลิตภัณฑ์และบริการที่ปลอดภัย เชื่อถือได้ เป็นมืออาชีพ และสอดคล้องตามกฎหมายเกี่ยวกับลูกค้า Tencent Cloud ยังกำหนดองค์ประกอบของเจ้าหน้าที่ประสานงานด้านความ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ามปลอดภัยข้อมูล (Information Security Liaison Officer) โดยเจ้าหน้าที่ประสานงานด้านความปลอดภัยข้อมูลในแต่ละภูมิภาคจะรักษาการสื่อสารที่ราบรื่นกับหน่วยงานกำกับดูแลท้องถิ่นและลูกค้าตามข้อกำหนดการปฏิบัติตามและความต้องการทางธุรกิจ เพื่อให้มั่นใจว่า Tencent Cloud ปฏิบัติตามกฎหมาย กฎระเบียบ และข้อตกลงตามสัญญา Tencent Cloud คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ให้บริการในงาน สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความปลอดภัย ระบบในงานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับในงานของลูกค้าผ่านกลไกการตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมและจัดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้าได้รับการตอบสนองและจัดการอย่างทันท่วงทีนอกจากนี้ Tencent Cloud ยังมีช่องทางออนไลน์และทางโทรศัพท์บนเว็บไซต์อย่างเป็นทางการ สนับสนุนให้ลูกค้าแสดงความคิดเห็นเกี่ยวกับปัญหาที่พบเมื่อใช้บริการ Tencent Cloud Tencent Cloud มีศูนย์บริการลูกค้าที่สำรองกันหลายภูมิภาค สามารถจัดการข้อซักถามหรือความต้องการจากลูกค้าได้อย่างต่อเนื่องตลอด 24 ชั่วโมงทุกวัน ให้การสนับสนุนทางเทคนิคที่มีคุณภาพสูงและตลอดเวลา ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับการสนับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า
2.2.3	การบริหารทรัพยากร พยาน สารสนเทศ	• มีการจัดทำรายการทรัพย์สินสารสนเทศและข้อมูลรายละเอียดของทรัพย์สิน สารสนเทศที่มีการจัดเก็บและประมวลผลอยู่บนระบบ Cloud Computing เป็นส่วนหนึ่งของรายการทรัพย์สิน	ลูกค้าควรจัดทำบัญชีรายการสินทรัพย์ข้อมูลและจำแนกประเภทและระดับสินทรัพย์ข้อมูลตามหลักการจำแนกประเภทและระดับของข้อมูล และทำการระบุ เพื่อช่วยเหลือลูกค้าในการบริหารสินทรัพย์ข้อมูลอย่างครอบคลุม Tencent Cloud Cloud Workload Protection Platform (CWPP)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		(Asset Inventory) ภายในกระบวนการบริหาร จัดการทรัพย์สินด้านเทคโนโลยีสาร สนเทศและกระบวนการที่เกี่ยวข้อง •ข้อมูลสารสนเทศและเอกสารที่มีกา รจัดเก็บบนระบบ Cloud Computing ควรได้รับการจัดชั้นความลับข้อมูลแ ลระบุประเภท (Labelling) ตามนโยบาย การจัดชั้นความลับข้อมูล	ซึ่งสนับสนุนการรวบรวมลายเซ็นดิจิทัลของสินทรัพย์โดย อัตโนมัติ และบริหารจัดการข้อมูลลายเซ็นดิจิทัลของสินทรัพย์ เช่น บัญชีผู้ใช้ พอร์ต กระบวนการ และแอปพลิเคชัน อย่างเป็นเอกภาพ CWPP ยังสามารถดำเนินการตรวจสอบอย่างรวดเร็วเกี่ยวกับขอ บเขตผลกระทบความเสี่ยงของเหตุการณ์ความปลอดภัย ที่เกิดขึ้นแล้ว ตามลายเซ็นดิจิทัลของสินทรัพย์ เพื่อช่วยลูกค้ายกระดับความปลอดภัยของเซิร์ฟเวอร์ ลูกค้ายังสามารถใช้แพลตฟอร์มการจัดการความปลอดภัย แบบครบวงจร Cloud Security Center (CSC) ของ Tencent Cloud เพื่อบริหารจัดการความปลอดภัยของสินทรัพย์ข้อมูล CSC มีฟังก์ชันศูนย์ความปลอดภัยสินทรัพย์ ซึ่งช่วยให้ลูกค้าสามารถตรวจนับสินทรัพย์บนคลาวด์แบบ ไดนามิกโดยอัตโนมัติ รวมถึงเซิร์ฟเวอร์คลาวด์ ที่เก็บวัตถุ ฐานข้อมูลคลาวด์ โหลดบาลานเซอร์ เป็นต้น และบริหารจัดการความเสี่ยงด้านความปลอดภัยของสิน ทรัพย์แบบครบวงจรผ่านหลายมิติความปลอดภัย เช่น ความเสี่ยงการกำหนดค่าคลาวด์ ช่องโหว่ และเหตุการณ์ความปลอดภัย เพื่อลดความเสี่ยง "IT ล่องหน" บนคลาวด์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ดูแล Tencent Cloud ได้กำหนดมาตรฐานการจัดการสินทรัพย์ข้อมูลและกระ บวนการจัดการตลอดวงจรชีวิตสินทรัพย์ เพื่อจัดการและปกป้องสินทรัพย์ เช่น ข้อมูลอิเล็กทรอนิกส์ ฮาร์ดแวร์และอุปกรณ์เสมือน โครงสร้างพื้นฐาน ระบบแอปพลิเคชัน และซอฟต์แวร์ โดยจำแนกประเภทและระดับ Tencent Cloud ใช้ระบบการจัดการสินทรัพย์ในการบริหารจัดการอุปกรณ์ ฮาร์ดแวร์และส่วนประกอบซอฟต์แวร์ รวมถึงการลงทะเบียนและผูกมัดสินทรัพย์ การตรวจนับและการอัปเดตข้อมูลสินทรัพย์ การปลดระวางและเปลี่ยนใหม่สินทรัพย์ เป็นต้น เพื่อรับประกันการทำงานที่ราบรื่นของระบบพื้นฐานของแ พลตฟอร์มคลาวด์ และจัดเตรียมการสนับสนุนที่เชื่อถือได้ให้กับระบบธุรกิจ เพื่อช่วยเหลือลูกค้าในการจัดประเภทและแปรรัด บข้อมูลบนระบบคอมพิวเตอร์คลาวด์ Data Security Governance Center (DSGC)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สามารถช่วยลูกค้าจัดการสินทรัพย์ข้อมูลโดยอัตโนมัติ จัดประเภทและประเมินความเสี่ยงด้านความปลอดภัยของข้อมูลขององค์กรบนคลาวด์ โดยได้รับอนุญาตจากองค์กร DSGC จะเชื่อมต่อกับสินทรัพย์ข้อมูลประเภทต่างๆ บนคลาวด์อย่างลึกซึ้ง และรับข้อมูลสินทรัพย์ข้อมูลที่ทันเวลาจากมิติภายใน ตามลักษณะของข้อมูล DSGC จะช่วยองค์กรค้นพบข้อมูลที่ละเอียดอ่อนอย่างเจาะจง และจัดระเบียบสินทรัพย์ข้อมูลจากมุมมองความปลอดภัย ตามมาตรฐานการจำแนกประเภทและระดับข้อมูลระดับชาติ อุตสาหกรรม หรือองค์กร DSGC จะช่วยองค์กรในการจำแนกประเภทและระดับข้อมูล โดยใช้วิธีการที่มองเห็นได้ ดูสถานะความปลอดภัยของสินทรัพย์จากหลายมิติ เช่น ภาพรวมสินทรัพย์ การจำแนกประเภทและระดับ สิทธิ์ของบัญชีผู้ใช้ การจัดเก็บข้อมูล และข้อมูลที่ละเอียดอ่อน Tencent Cloud ได้สร้างมาตรฐานการจำแนกประเภทและระดับข้อมูลที่สมบูรณ์ภายในองค์กร โดยข้อมูลทั้งหมดจะถูกจำแนกประเภทและระดับตามมาตรฐานนี้เป็นเอกภาพตั้งแต่เริ่มสร้าง ข้อมูลของลูกค้าภายใน Tencent Cloud จัดอยู่ในระดับความปลอดภัยสูง สำหรับพนักงานภายใน Tencent Cloud หากไม่ใช้บริการที่ลูกค้าเลือกใช้ซึ่งจำเป็นต้องประมวลผลข้อมูลของลูกค้า พนักงาน Tencent Cloud จะไม่พยายามเข้าถึงข้อมูลลูกค้าใดๆ
2.2.3	การควบคุมการเข้าถึง	- มีการกำหนดการควบคุมการเข้าถึงและสิทธิ์การใช้งานและบริการทางเครือข่ายของ ระบบให้บริการ Cloud Computing ที่มีการใช้งาน - มีการใช้วิธีพิสูจน์ตัวตนที่เหมาะสม เช่น การใช้งาน multi-factor authentication สำหรับการเข้าถึงฟังก์ชันการบริหารระบบ (Administrator page) - มีการตรวจสอบวิธีและขั้นตอนการส่งมอบรหัสผ่าน (Secret	ลูกค้าควรสร้างกลไกการพิสูจน์ตัวตนและการควบคุมการเข้าถึงสำหรับระบบบริการคอมพิวเตอร์คลาวด์ เพื่อควบคุมการเข้าถึงสินทรัพย์ข้อมูล ทบทวนและอัปเดตสิทธิ์เป็นประจำ และเสริมสร้างการจัดการความปลอดภัยของบัญชีผู้ใช้ที่มีสิทธิ์พิเศษและซอฟต์แวร์ยูทิลิตี้ (utility software) โดยใช้การพิสูจน์ตัวตนหลายปัจจัยและกลไกการตรวจสอบ เป็นต้น ลูกค้ายังควรกำหนดนโยบายรหัสผ่านที่แข็งแกร่งสำหรับระบบคอมพิวเตอร์คลาวด์ ในด้านการจัดการบัญชีผู้ใช้และการให้สิทธิ์ Cloud Access Management (CAM)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		authentication information) ของการใช้งานระบบ Cloud Computing ของผู้ให้บริการ อย่างปลอดภัย	สามารถช่วยลูกค้าจัดการการเข้าถึงผลิตภัณฑ์และบริการของ Tencent Cloud ได้อย่างปลอดภัยและละเอียดรอบคอบ
		•มีการตรวจสอบความสามารถในการบริหารจัดการและกำหนดสิทธิ์การเข้าถึงข้อมูล และบริการที่อยู่บนระบบ Cloud Computing ได้ตามแนวทางและนโยบายการควบคุมการเข้าถึง เช่น การกำหนดสิทธิ์การเข้าถึงบริการ การกำหนดสิทธิ์การเข้าถึงฟังก์ชันตามอำนาจหน้าที่ความรับผิดชอบ การกำหนดสิทธิ์การเข้าถึงข้อมูล เป็นต้น	Tencent Cloud ยังได้กำหนดกลยุทธ์การให้สิทธิ์การควบคุมการเข้าถึงและกลไกเมทริกซ์การแบ่งแยกสิทธิ์ภายในองค์กร Tencent Cloud ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการตรวจสอบสิทธิ์การเข้าถึงของพนักงาน โดยผู้ใช้งานต้องผ่านการยืนยันตัวตนสองปัจจัยก่อนเข้าถึงทรัพยากรภายใน Tencent Cloud
		•มีการตรวจสอบแนวทางการควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Utility Program) ในการเข้าถึงและบริหารจัดการระบบ Cloud Computing (ถ้ามี)	ปฏิบัติตามหลักการสิทธิ์น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิ์น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิ์เฉพาะก็ต่อเมื่อมีความจำเป็นต้องใช้ และผ่านกระบวนการอนุมัติสิทธิ์ที่เข้มงวดเท่านั้น
			Tencent Cloud จะรักษาด่านที่กั้นข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดการตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์
			สำหรับผู้ใช้งานที่มีสิทธิ์สูง Tencent Cloud มี Bastion Host (BH) ที่สามารถรองรับการให้สิทธิ์อย่างละเอียดตามมิติต่าง ๆ เช่น ผู้ใช้ สินทรัพย์ บัญชี และสิทธิ์การดำเนินงาน เพื่อให้มั่นใจว่าสิทธิ์ที่ผู้ใช้งานมีอยู่เป็นสิทธิ์ขั้นต่ำที่จำเป็นสำหรับการเข้าถึงสินทรัพย์และทำงานให้สำเร็จ
			สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้เครื่องบินคุ้มกัน อย่างเต็มรูปแบบ โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบแบ็กเอนด์จากส่วนกลางผ่าน เครื่องบินคุ้มกัน การเข้าถึงเครื่องบินคุ้มกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติสิทธิ์ มีเฉพาะเจ้าหน้าที่ปฏิบัติการภายในของ Tencent Cloud บางส่วนเท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบ เครื่องบินคุ้มกัน ต้องการการยืนยันตัวตนสองปัจจัย
			บันทึกการดำเนินการปฏิบัติงานแบ็กเอนด์ทั้งหมดจะถูกเก็บไว้โดยศูนย์กลางแพลตฟอร์มบันทึก (log) และได้รับการตรวจสอบโดยทีมตรวจสอบภายในของ Tencent Cloud เป็นประจำ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สำหรับการลงทะเบียนและการใช้บัญชีลูกค้า ในกระบวนการลงทะเบียนบัญชี ลูกค้าจำเป็นต้องอ่านและยอมรับ "ข้อตกลงบริการ Tencent Cloud" บนเว็บไซต์อย่างเป็นทางการของ Tencent Cloud ซึ่งข้อตกลงดังกล่าวกำหนดความรับผิดชอบและหน้าที่ที่ เกี่ยวข้องกับการจัดการการเข้าถึงของลูกค้า คอนโซลการจัดการเป็นศูนย์กลางสำหรับลูกค้าในการ จัดการและควบคุมทรัพยากรคลาวด์ เมื่อลูกค้าลงทะเบียนบัญชีคลาวด์ คอนโซลการจัดการจะตรวจสอบความเป็นเอกลักษณ์ของ ชื่อบัญชีผู้ใช้โดยอัตโนมัติ เมื่อลูกค้าเข้าสู่ระบบคอนโซลการจัดการ ข้อมูลการพิสูจน์ตัวตนจะถูกส่งผ่านโปรโตคอล HTTPS ลูกค้าสามารถจัดการบริการและข้อมูลคลาวด์แบบรวมศูนย์ ผ่าน API ที่เปิดเผย เมื่อลูกค้าลงทะเบียนฟังก์ชัน Open API ลูกค้าจำเป็นต้องใช้วิธีการเข้าถึงที่จัดสรรให้แก่ลูกค้าแต่ละ รายเพื่อการพิสูจน์ตัวตน ก่อนเข้าถึงบริการคลาวด์ ตัวตนของลูกค้าจะผ่านการพิสูจน์ตัวตนโดยใช้วิธีการเข้าถึง ของลูกค้า ลูกค้าสามารถใช้การพิสูจน์ตัวตนหลายปัจจัยเพื่อเพิ่มความ ปลอดภัยสำหรับการเข้าสู่ระบบบัญชีและการดำเนินการ ที่ละเอียดอ่อนใดๆ (เช่น การเปลี่ยนรหัสผ่านบัญชี) ของตน
2.2.3	การเข้ารหัส	- มีการใช้งานเทคโนโลยีการเข้ารหัสที่สอดคล้องกับความเสี่ยงในกระบวนการรับส่ง และจัดเก็บข้อมูลบนระบบ Cloud Computing - ทั้งในกรณีที่มีการดำเนินการโดยผู้ประกอบการธุรกิจ หรือดำเนินการโดยผู้ให้บริการ - มีการควบคุมและจัดการกุญแจการเข้ารหัส (Cryptographic key) ที่มีการใช้งานในระบบ Cloud Computing ให้เป็นตามนโยบายและกระบวนการบริหารจัดการกุญแจ การเข้ารหัส - กรณีการบริหารจัดการกุญแจและการเข้ารหัสดำเนินการโดยผู้ให้บริการผู้ประกอบการธุรกิจ	ลูกค้าควรใช้อัลกอริทึมการเข้ารหัสตามมาตรฐานสากล และสร้างนโยบาย มาตรฐาน และขั้นตอนการจัดการคีย์รหัสผ่านที่ครอบคลุมขั้นตอนต่างๆ เช่น การสร้าง การแจกจ่าย การติดตั้ง การอัปเดต การเพิกถอน การกู้คืน และการหมดอายุของคีย์รหัสผ่าน นอกจากนี้ ลูกค้าควรกำหนดมาตรการควบคุมสำหรับคีย์รหัสผ่านที่จัดเตรียมโดยบุคคลภายนอกให้ชัดเจน และจัดทำขั้นตอนการจัดการเหตุการณ์การรั่วไหลของคีย์รหัสผ่าน ในด้านการป้องกันการจัดเก็บข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริทึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสานรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		รวบรวมข้อมูลและแนวทางการจัดการกฎและการเข้ารหัสที่อยู่ในความดูแลของ	รับประกันความเป็นความลับของข้อมูล ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เน็ต Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจถึงความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า ในด้านการจัดการคีย์ Tencent Cloud ยังได้กำหนดมาตรฐานการเข้ารหัสและการจัดการคีย์ โดยกำหนดข้อกำหนดด้านความปลอดภัยสำหรับกระบวนการต่างๆ ในการสมัครคีย์ การสร้าง การจัดเก็บ การใช้ การส่งต่อ การอัปเดต และการทำลายคีย์ การดำเนินการต่างๆ ที่เกี่ยวข้องกับวงจรชีวิตของคีย์ทั้งหมดต้องปฏิบัติตามข้อกำหนดพื้นฐานของการควบคุมสองชั้น การส่งมอบที่เข้มงวด การเก็บรักษาที่เหมาะสม และการอัปเดตที่ทันเวลาที่กระบวนการใช้คีย์ยังต้องแน่ใจว่าปฏิบัติตามข้อกำหนด เช่น การแยกหน้าที่และความรับผิดชอบ การอนุมัติที่เข้มงวด และการดำเนินการด้วยข้อจริง และต้องเก็บรักษาบันทึกการดำเนินการคีย์ทางธุรกิจ และดำเนินการตรวจสอบการดำเนินการเป็นประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการเทคโนโลยีการเข้ารหัส โปรดดูเนื้อหาในข้อ "6 การควบคุมการเข้ารหัส" ของ " 11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ " ในคู่มือนี้
2.2.3	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	ผู้ประกอบธุรกิจควรสอบทานนโยบายและแนวทางการทำลาย (Dispose) และการนำกลับมาใช้ (Reuse) ของอุปกรณ์หรือทรัพยากรด้านสารสนเทศของผู้ให้บริการ	ลูกค้าควรตรวจสอบให้แน่ใจว่าข้อมูลในอุปกรณ์หรือทรัพยากรเทคโนโลยีสารสนเทศ สื่จัดเก็บข้อมูล ระบบ และอุปกรณ์ปลายทาง ได้ถูกลบอย่างถาวรไม่สามารถกู้คืนได้ก่อนที่จะดำเนินการจำหน่ายหรือนำไปใช้งานใหม่ Tencent Cloud รักษาบัญชีรายละเอียดของฮาร์ดแวร์และสิ่งอำนวยความสะดวกในฐานข้อมูลการจัดการการกำหนดค่า (Configuration Management Database: CMDB)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ซึ่งรวมถึงวันที่สิ้นสุดการสนับสนุน (End-of-Support Date) และข้อมูลเวอร์ชันของแพลตฟอร์มสำหรับแต่ละเซิร์ฟเวอร์ Tencent Cloud ดำเนินการปลดระวางและเปลี่ยนเซิร์ฟเวอร์เป็นประจำ ส่วนประกอบประเภทซอฟต์แวร์ (เช่น ระบบปฏิบัติการและระบบฐานข้อมูล) จะถูกเปลี่ยนเป็นเวอร์ชันที่เหมาะสมก่อนวันที่สิ้นสุดการสนับสนุน สำหรับฮาร์ดแวร์ที่ปลดระวางแล้ว Tencent Cloud ใช้วิธีการทำลายทางกายภาพที่ปลอดภัยเพื่อรับประกันว่าฮาร์ดแวร์ถูกทำลายอย่างสมบูรณ์และมีการบันทึกการไว้ในบันทึกการทำลาย สำหรับการลบและทำลายข้อมูล Tencent Cloud มีกลไกทำลายข้อมูลที่ปลอดภัยและเชื่อถือได้ เมื่อบริการของลูกค้าหมดอายุลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรองอย่างสิ้นเชิงหลังช่วงเวลาเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้ เมื่อสื่อที่ใช้ให้บริการ Tencent Cloud เกิดความขัดข้องและจำเป็นต้องเปลี่ยนหรือถึงอายุการใช้งานและจำเป็นต้องกำจัด Tencent Cloud จะลบข้อมูลที่เหลืออยู่ทันที และปฏิบัติตามขั้นตอนที่เข้มงวดเพื่อทำลายทางกายภาพอย่างสมบูรณ์ในเวลาที่เหมาะสม
2.2.3	การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน	• ผู้ประกอบธุรกิจควรกำหนดแนวทางการบริหารการแก้ไขเปลี่ยนแปลงที่ครอบคลุม • ผลกระทบจากการแก้ไขเปลี่ยนแปลงอันอาจเกิดขึ้นจากผู้ให้บริการ • ผู้ประกอบธุรกิจควรมีการติดตามการแก้ไขเปลี่ยนแปลงใด ๆ • อันอาจมีการดำเนินการโดยผู้ให้บริการ - รวมถึงการประเมินผลกระทบจากกรณี • ในกรณีมีข้อตกลงให้ผู้ให้บริการมีความรับผิดชอบในกิจกรรมการสำรองข้อมูล - ผู้ประกอบธุรกิจควรดำเนินการสอบ	ลูกค้าควรกำหนดขั้นตอนและกลไกสำหรับการจัดการการเปลี่ยนแปลง การจัดการการสำรองข้อมูล การจัดการบันทึกเหตุการณ์ และการจัดการช่องโหว่และแพตช์ ลูกค้าควรประเมินผลกระทบของการเปลี่ยนแปลงที่เป็นไปได้ใดๆ สำรองข้อมูลเป็นประจำ บันทึกและป้องกันบันทึกเหตุการณ์ที่เกี่ยวข้องกับระบบบริการคอมพิวเตอร์คลาวด์และบันทึกกิจกรรมการจัดการระบบ นอกจากนี้ ควรประเมินสถานการณ์การจัดการช่องโหว่และแพตช์ของผู้ให้บริการเป็นประจำ ในด้านการจัดการการเปลี่ยนแปลง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานการจัดการสำหรับการเปลี่ยนแปลงผลิตภัณฑ์และการกำหนดค่าที่กำหนดขั้นตอนต่างๆ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ทานขั้นตอนและแนวทางการสำรองข้อมูล ที่ดำเนินการโดยผู้ให้บริการให้มีความสอดคล้องกับนโยบายการสำรองข้อมูล ของผู้ประกอบการธุรกิจ • ในกรณีไม่มีข้อตกลงให้ผู้ให้บริการดำเนินการสำรองข้อมูล ผู้ประกอบการธุรกิจควรจัดให้มีกระบวนการสำรองข้อมูลอย่างเพียงพอ และสอดคล้องกับนโยบายการสำรองข้อมูล • ผู้ประกอบการธุรกิจควรกำหนดความต้องการทางด้านการจัดเก็บบันทึกเหตุการณ์ ที่เกี่ยวข้องกับระบบให้บริการ Cloud Computing และตรวจสอบการดำเนินการจัดเก็บบันทึกเหตุการณ์ของผู้ให้บริการ • กรณีกิจกรรมการบริหารจัดการระบบ (Privileged Operation) อยู่ภายใต้ความรับผิดชอบของผู้ประกอบการ ผู้ประกอบการควรประเมินความเสี่ยงของการจัดเก็บบันทึกเหตุการณ์ที่เกี่ยวข้องกับกิจกรรมการบริหารจัดการระบบ และ/หรือ ประเมินความจำเป็นในการดำเนินการมาตรการเพิ่มเติมเพื่อจัดเก็บและรักษาความปลอดภัยบันทึกเหตุการณ์ดังกล่าว • ผู้ประกอบการธุรกิจควรตรวจสอบแนวทางในการเทียบเวลา (Clock synchronization) ของผู้ให้บริการ • ผู้ประกอบการธุรกิจควรตรวจสอบและประเมินแนวทางการบริหารจัดการช่องโหว่ และ	ในกระบวนการเปลี่ยนแปลงและผู้รับผิดชอบที่เกี่ยวข้องอย่างชัดเจน เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการอนุมัติและทดสอบอย่างเหมาะสมก่อนการดำเนินการ ในเวลาเดียวกัน Tencent Cloud ได้กำหนดขั้นตอนการจัดการสำหรับการเปลี่ยนแปลงฉุกเฉิน โดยการเปลี่ยนแปลงฉุกเฉินต้องได้รับการอนุมัติที่เหมาะสมก่อนจึงจะสามารถดำเนินการได้ การเปลี่ยนแปลงโปรแกรมทุกประเภท รวมถึงการเปลี่ยนแปลงแอปพลิเคชันและไฟล์กำหนดค่าระบบปฏิบัติการ และฐานข้อมูล ต้องได้รับการวิเคราะห์ผลกระทบทางธุรกิจก่อนการเปิดตัว จัดทำแผนย้อนกลับสำหรับการเปลี่ยนแปลง และได้รับการอนุมัติจากผู้รับผิดชอบที่เกี่ยวข้อง ระบบเผยแพร่การเปลี่ยนแปลงของ Tencent Cloud บังคับให้การดำเนินการเปลี่ยนแปลงสามารถดำเนินการได้ดีโดยบุคคลที่ได้รับอนุญาตเท่านั้น และเก็บรักษาบันทึกที่เกี่ยวข้องกับการเปลี่ยนแปลงไว้ พร้อมทั้งตรวจสอบบันทึกเป็นประจำ หลังการเผยแพร่การเปลี่ยนแปลง Tencent Cloud จะตรวจสอบ ตรวจสอบ และบันทึกผลการเปลี่ยนแปลงในสภาพแวดล้อมการผลิต Tencent Cloud จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอการดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน และขอบเขตของการเปลี่ยนแปลง สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแวดล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขยาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการเปลี่ยนแปลง โปรดดูเนื้อหาในข้อ "8.2 การบริหารจัดการการเปลี่ยนแปลง" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		การติดตั้งชุดโปรแกรมแก้ไข (Patch) ของผู้ให้บริการ	ในด้านการจัดการการสำรองข้อมูล ในเวลาเดียวกัน Tencent Cloud ได้สร้างหรือเข้าศูนย์ข้อมูลในหลายพื้นที่ทั่วโลกตามมาตรฐานสากลที่เกี่ยวข้องและข้อกำหนดความปลอดภัยในท้องถิ่น เพื่อมอบตัวเลือกภูมิภาคและโซนความพร้อมใช้งานหลายแห่งให้แก่ลูกค้า เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติและระดับการบริการของธุรกิจ ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud ให้มา เช่น บริการคอมพิวเตอร์ บริการเครือข่าย บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ ไม่เพียงแต่สามารถจัดเตรียมสถาปัตยกรรมระบบที่มีความพร้อมใช้งานสูงให้แก่ลูกค้า แต่ยังสนับสนุนให้ลูกค้ากำหนดกลยุทธ์การสำรองข้อมูลสำหรับระบบและข้อมูลของตนเอง ตอบสนองความต้องการสำรองข้อมูลทุกประเภทของลูกค้า สำหรับข้อมูลของลูกค้าที่จัดเก็บไว้บนคลาวด์ Tencent Cloud ใช้วิธีการสำรองข้อมูลแบบเรียลไทม์ การเก็บข้อมูลสำรองหลายชุด และการสำรองข้อมูลข้ามพื้นที่ เพื่อรับประกันความปลอดภัยและความน่าเชื่อถือของข้อมูลธุรกิจที่ลูกค้าเก็บไว้บนคลาวด์ รวมถึงความพร้อมใช้งานอย่างต่อเนื่อง Tencent Cloud ยังใช้มาตรการป้องกันหลายประการ เช่น ความปลอดภัยทางกายภาพ การควบคุมการเข้าถึง การแยกทางตรรกะ และสนับสนุนให้ลูกค้าใช้ Key Management Service (KMS) และ Cloud Access Management (CAM) เพื่อป้องกันไม่ให้ข้อมูลสำรองของลูกค้าถูกเข้าถึงหรือแก้ไขโดยไม่ได้รับอนุญาต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการสำรองข้อมูล โปรดดูเนื้อหาในข้อ "8.6 การสำรองข้อมูล" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในคู่มือนี้" ในด้านการจัดการบันทึก Tencent Cloud ให้บริการ Cloud Log Service (CLS) เพื่อช่วยเหลือผู้ใช้ในการแก้ไขปัญหาด้านการดำเนินงาน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			กิจ การตรวจสอบความปลอดภัย การตรวจสอบบันทึก และการวิเคราะห์บันทึกผ่านบันทึก Tencent Cloud CLS ใช้การออกแบบสถาปัตยกรรมแบบกระจายที่มีความพร้อมใช้งานสูง จัดเก็บข้อมูลบันทึกด้วยการสำรองข้อมูลหลายชุด ป้องกันไม่ให้ข้อมูลไม่สามารถใช้งานได้เมื่อบริการไหนเดิ ยวขัดข้อง ให้บริการที่มีความพร้อมใช้งานสูง และรับประกันบริการที่เสถียรและน่าเชื่อถือสำหรับข้อมูล บันทึก ด้วย CloudAudit ผู้ใช้สามารถบันทึกบันทึก ตรวจสอบอย่างต่อเนื่อง และเก็บรักษากิจกรรมบัญชีที่เกี่ยวข้องกับการดำเนินการ ในโครงสร้างพื้นฐาน Tencent Cloud ทั้งหมด ลูกค้าสามารถใช้บริการ Elasticsearch Service (ES) เพื่อรวบรวมและส่งบันทึกแบบเรียลไทม์ของเซิร์ฟเวอร์คลาวด์ คอนเทนเนอร์ และผลิตภัณฑ์คลาวด์อื่นๆ หรือข้อมูลธุรกิจที่มีอยู่และเพิ่มขึ้นของธุรกิจ ไปยังคลัสเตอร์ ES ของ Tencent Cloud เพื่อจัดเก็บข้อมูลแบบกระจาย และการสืบค้นและการวิเคราะห์ข้อมูล เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะรวบรวมบันทึกต่างๆ เช่น บันทึกการเข้าสู่ระบบ บันทึกการดำเนินการ บันทึกระบบทั่วไป และบันทึกเหตุการณ์ความปลอดภัยของระบบ ไปยังแพลตฟอร์มการจัดการบันทึกของ Tencent Cloud อย่างเป็นเอกภาพ และใช้มาตรการสำรองข้อมูลและการป้องกันที่เข้มงวดสำหรับข้อมูลบันทึกที่เกี่ยวข้อง เพื่อป้องกันการแก้ไขและการลบโดยไม่ได้รับอนุญาต Tencent Cloud ดำเนินการตรวจสอบบันทึกผ่านเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติการและทีมตรวจสอบภายใน เพื่อตรวจสอบความผิดปกติของระบบหรือการดำเนินการ เพื่อป้องกันความเสี่ยงในการปฏิบัติการ Tencent Cloud รับประกันว่านาฬิกาของสิ่งอำนวยความสะดวกที่เกี่ยวข้อง ซึ่งโครโนซ์กับแหล่งเวลาที่แม่นยำ และศูนย์ข้อมูลแต่ละแห่งจะตรวจสอบสถานะการซิงโครไนซ์เวลาของเซิร์ฟเวอร์ NTP ของตนเป็นประจำ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการบันทึก โปรดดูเนื้อหาในข้อ "8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยว กับระบบ IT (log)" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ " ในคู่มือนี้ ในด้านการจัดการช่องโหว่และแพตช์ ลูกค้ายังสามารถใช้ Cloud Workload Protection Platform (CWPP) เพื่อตรวจจับช่องโหว่ซอฟต์แวร์ Linux ช่องโหว่ระบบปฏิบัติการ Windows ช่องโหว่ Web-CMS และช่องโหว่แอปพลิเคชัน แจ้งเตือนแบบเรียลไทม์ และรับโซลูชันการแก้ไขช่องโหว่ ช่วยลูกค้าตอบสนองต่อความเสี่ยงจากช่องโหว่อย่างรวดเร็ว ริ้ว Tencent Container Security Service (TCSS) เป็นระบบแพตช์เสมือนที่ Tencent Cloud Security พัฒนาขึ้นเพื่อป้องกันช่องโหว่วันศูนย์ (zero- day) ที่เกิดขึ้นบ่อยครั้ง ซึ่งผสมรวมเทคโนโลยีการขุดเจาะช่องโหว่และการแจ้งเตือน ช่องโหว่ร้ายแรงแบบเรียลไทม์ของ Tencent ใช้เพื่อตรวจจับและวิเคราะห์ช่องโหว่ สร้างแพตช์เสมือนตามความรู้ความเชี่ยวชาญของ Tencent และทำให้แพตช์เสมือนมีผลบนเซิร์ฟเวอร์คลาวด์โดยอัตโนมัติ เพื่อป้องกันการโจมตีของแฮกเกอร์ได้อย่างมีประสิทธิภาพ นอกจากนี้ ลูกค้ายังสามารถใช้ Vulnerability Scanning Service (VSS) เพื่อดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของอุปกรณ์เครือข่ายและบริการแอป พลิเคชันขององค์กร และใช้คำแนะนำการแก้ไขที่มีอาชีพจาก VSS เพื่อลดความเสี่ยงด้านความปลอดภัยขององค์กร เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ดูแล ในด้านการจัดการแพตช์ Tencent Cloud จะระบุแพตช์ล่าสุด และดำเนินการทดสอบความปลอดภัยอย่างเพียงพอก่อน การติดตั้งแพตช์ เพื่อให้มั่นใจในความปลอดภัยของการติดตั้งแพตช์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Tencent Cloud จะแจ้งให้ทีมงานธุรกิจภายในแต่ละทีมทราบเป็นประจำเกี่ยวกับการอัปเดตและติดตั้งแพตช์ และใช้เครื่องมือตรวจสอบจุดปลายทาง (endpoint) สแกนสถานะการติดตั้งแพตช์เป็นประจำ และอุปกรณ์ที่ไม่ได้ติดตั้งแพตช์เกินกำหนดเวลาจะถูกสร้างในงานแจ้งเตือนโดยอัตโนมัติ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการช่องโหว่และแพตช์ โปรดดูเนื้อหาในข้อ "8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้
2.2.3	ความมั่นคงปลอดภัยของการสื่อสารข้อมูล	• ผู้ประกอบธุรกิจควรประเมินและกำหนดความต้องการทางการแบ่งแยกเครือข่ายและสภาพแวดล้อมการใช้งาน Cloud (Tenant isolation) ในสภาพแวดล้อมที่มีการใช้งานร่วมกัน (Multi-tenant) และตรวจสอบการดำเนินการของผู้ให้บริการตาม ข้อตกลงการให้บริการ	สถาบันการเงินควรประเมินและกำหนดความต้องการในการแบ่งส่วนเครือข่ายและการแยกผู้เช่าในสภาพแวดล้อมคลาวด์ และตรวจสอบพฤติกรรมของผู้ให้บริการตามข้อตกลงการให้บริการ สำหรับข้อกำหนดการแบ่งส่วนเครือข่าย ลูกค้าสามารถใช้บริการ Virtual Private Cloud (VPC) ที่ Tencent Cloud ให้มาเพื่อสร้างพื้นที่เครือข่ายอิสระหลายแห่งสำหรับทรัพยากรแพลตฟอร์มคลาวด์ที่ได้ซื้อไปแล้ว และกำหนดการแบ่งส่วนเครือข่ายและที่อยู่ IP นโยบายการกำหนดเส้นทาง ฯลฯ ตามต้องการได้ด้วยตนเอง บริการ VPC เป็นพื้นที่เครือข่ายบนคลาวด์เฉพาะที่สร้างขึ้นบน Tencent Cloud โดยเครือข่ายส่วนตัวใช้เทคโนโลยีโมดูล สร้างเครือข่ายเสมือนบนเครือข่ายกายภาพ และใช้เทคโนโลยีเสมือนจริง เพื่อให้บรรลุการแยกอินทราเน็ตโดยสมบูรณ์ระหว่างเครือข่ายส่วนตัวต่างๆ มอบเครือข่ายคลาวด์ที่ปลอดภัยเป็นอิสระและแยกจากกันให้กับลูกค้า สำหรับเซิร์ฟเวอร์คลาวด์ภายในเครือข่ายส่วนตัว สามารถควบคุมการไหลเข้าออกของข้อมูลในระดับอินสแตนซ์และซับเน็ตได้ผ่านการกำหนดค่ากลุ่มความปลอดภัยและกฎ Access Control List (ACL) ของเครือข่าย เพื่อให้บรรลุการควบคุมการเข้าถึงเครือข่ายในระดับต่างๆ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สำหรับการแยกหลายผู้เช่า (Multi-tenancy Isolation) Tencent Cloud มีกลไกความปลอดภัย เช่น นโยบายการควบคุมการเข้าถึงทรัพยากรในชั้นควบคุมเสมือน (Virtualization Control Layer) นโยบายการแยกระหว่างเครือข่ายส่วนตัวภายในแพลตฟอร์มคลาวด์ การจัดสรรสิทธิ์และการยืนยันตัวตนบนเว็บคอนโซล รหัสเซสชันของอินเทอร์เน็ตเฟส และคีย์การเข้าถึง เพื่อให้มั่นใจว่าผู้ใช้แต่ละคนสามารถเข้าถึงทรัพยากรคอมพิวเตอร์คลาวด์ที่ตนซื้อได้เท่านั้น ซึ่งทำให้เกิดการแยกการเข้าถึงระหว่างผู้เช่าหลายรายได้อย่างมีประสิทธิภาพ ในด้านการจัดการควบคุมความปลอดภัยเครือข่าย Tencent Cloud ยังได้สร้างมาตรฐานการจัดการความปลอดภัยเครือข่ายและระบบป้องกันเครือข่ายแบบหลายชั้นภายในองค์กร Tencent Cloud กำหนดมาตรฐานการควบคุมและป้องกันความปลอดภัยเครือข่าย ตลอดจนบทบาทและความรับผิดชอบที่เกี่ยวข้องอย่างชัดเจนผ่านระบบการจัดการและขั้นตอนการทำงาน เพื่อให้มั่นใจว่ากิจกรรมที่ดำเนินการบนเครือข่ายของ Tencent Cloud ดำเนินไปอย่างปลอดภัย ในเวลาเดียวกัน Tencent Cloud ได้ปรับใช้สถาปัตยกรรมความปลอดภัยเครือข่ายที่ครบถ้วน โดยใช้กลไกการป้องกันหลายชั้น เช่น ไฟร์วอลล์ ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) การป้องกัน DDoS การแยกทางลอจิกของเครือข่าย และความปลอดภัยของแอปพลิเคชันเว็บ เพื่อตรวจจับกรอง และบล็อกการรับส่งข้อมูลเครือข่ายที่เป็นอันตรายได้ทันที่ ปกป้องความปลอดภัยเครือข่ายของ Tencent Cloud นอกจากนี้ Tencent Cloud ใช้มาตรการต่างๆ เช่น การควบคุมสิทธิ์และการอนุมัติขั้นตอน เพื่อห้ามไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงทรัพยากรเครือข่ายภายใน ซึ่งรวมถึงเครื่องมือวิเคราะห์และตรวจสอบเครือข่าย สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความปลอดภัยในการสื่อสาร โปรดดูเนื้อหาในข้อ "9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร ของ "11.3 ภาคผนวก 3

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			<u>การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ</u> " ในคู่มือนี้
2.2.3	การจัดการ พัฒนา และดูแลรักษา ระบบสารสนเทศ	• ผู้ประกอบธุรกิจควรดำเนินการประเมินความต้องการด้านการรักษาความมั่นคง ปลอดภัยสารสนเทศของการใช้งาน Cloud Computing พร้อมทั้งประเมินและตรวจสอบความสามารถของผู้ให้บริการ cloud • เป็นส่วนหนึ่งในกิจกรรมการประเมินและคัดเลือกผู้ให้บริการ (Due Diligence) • กรณีการใช้งานในรูปแบบ SaaS ผู้ประกอบการควรประเมินและตรวจสอบผู้ให้บริการ • ด้านการจัดให้มีขั้นตอนและแนวทางการพัฒนาระบบอย่างปลอดภัย (Secure development procedure)	ลูกค้าควรใช้ข้อกำหนดความปลอดภัยข้อมูลที่ใช้ในการประมวลผลบนคลาวด์เป็นส่วนหนึ่งของการประเมินความสามารถของผู้ให้บริการในระหว่างกระบวนการตรวจสอบอย่างละเอียดของผู้ให้บริการคลาวด์ หากลูกค้าใช้รูปแบบ SaaS ควรประเมินกระบวนการพัฒนาระบบความปลอดภัยของผู้ให้บริการคลาวด์ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์อิงตามความต้องการของลูกค้าได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองต่อการตรวจสอบอย่างละเอียดของลูกค้าสำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบอย่างละเอียดสามารถอ้างอิงเนื้อหาในภาคผนวก 3-2 " การคัดเลือกผู้ให้บริการภายนอก" ของบทที่ 6 "Tencent Cloud จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับหลักเกณฑ์การใช้บริการจากผู้ให้บริการภายนอก ของ BOT อย่างไร" ได้อย่างไร" ในคู่มือนี้ ในด้านการจัดการวงจรชีวิตการพัฒนาระบบความปลอดภัย Tencent Cloud ยังได้สร้างมาตรฐานการพัฒนาความปลอดภัยระบบสารสนเทศภายในองค์กร และมุ่งมั่นพัฒนาตามมาตรฐาน ISO/IEC 20000 การจัดการบริการเทคโนโลยีสารสนเทศ ระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001 และมาตรฐานระบบการจัดการคุณภาพ ISO/IEC 9001 เข้ากับกระบวนการวงจรชีวิตการพัฒนาความปลอดภัยผลิตภัณฑ์ทั้งหมด ให้ความสำคัญกับขั้นตอนต่างๆ เช่น ความต้องการ การออกแบบ การวิจัยและพัฒนา การทดสอบ การส่งมอบ และการดำเนินการและบำรุงรักษา ผสานแนวคิดด้านความปลอดภัยข้อมูลและการปกป้องความเป็นส่วนตัวเข้าไปในแต่ละขั้นตอนของการพัฒนาผลิตภัณฑ์ เพื่อให้มั่นใจว่าผลิตภัณฑ์คลาวด์ได้รับความควบคุมด้านความปลอดภัยที่เพียงพอตลอดวงจรชีวิตของผลิตภัณฑ์ มาตรการควบคุมความปลอดภัยที่เกี่ยวข้อง ได้แก่:

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			การฝึกอบรมความปลอดภัย: ส่งเสริมจิตสำนึกการเขียนโปรแกรมที่ปลอดภัยสำหรับนักพัฒนา กำหนดให้นักพัฒนาปฏิบัติตามมาตรฐานการเข้ารหัสที่ปลอดภัยอย่างเคร่งครัด การวิเคราะห์ความต้องการ: สื่อสารเกี่ยวกับเนื้อหาและกระบวนการธุรกิจและกรอบทางเทคนิค เพื่อค้นหาวิธีที่ดีที่สุดในการฝังความปลอดภัย การออกแบบระบบ: สร้างแบบจำลองภัยคุกคามสำหรับการออกแบบระบบ และประเมินความปลอดภัยทางเทคนิคของสถาปัตยกรรมที่ใช้ การพัฒนาแบบ: ในระหว่างกระบวนการพัฒนา จัดเตรียมส่วนประกอบการพัฒนาความปลอดภัยที่ Tencent ออกแบบเองสำหรับนักพัฒนาใช้ และเขียนโค้ดตามมาตรฐานการเข้ารหัสความปลอดภัยของ Tencent Cloud การยืนยันความปลอดภัย: ค้นพบช่องโหว่ผ่านการตรวจสอบความปลอดภัยของโค้ด การสแกนความปลอดภัยของสินทรัพย์ การสแกนเว็บ การประเมินความปลอดภัยด้วยมนุษย์ การทดสอบเจาะระบบ และการตรวจสอบโค้ด การเผยแพร่: ระบบจะเผยแพร่ไปยังสภาพแวดล้อมออนไลน์ได้ก็ต่อเมื่อความเสี่ยงสูงทั้งหมดได้รับการแก้ไขแล้ว เพื่อป้องกันไม่ให้เกิดผลกระทบในการทำงานในสภาพแวดล้อมการผลิตโดยมีช่องโหว่ด้านความปลอดภัย
2.2.3	การบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ	- มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบในกระบวนการบริหารจัดการ - เหตุการณ์อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างชัดเจน - ระหว่างผู้ประกอบการธุรกิจและผู้ให้บริการ - มีการกำหนดช่องทางการติดต่อแล	ลูกค้าควรกำหนดหน้าที่และความรับผิดชอบระหว่างตนเองกับผู้ให้บริการให้ชัดเจนเมื่อเกิดเหตุการณ์ด้านความปลอดภัยของระบบสารสนเทศ และควรสร้างแผนการสื่อสารรายงานเหตุการณ์ความปลอดภัย พร้อมจัดทำกลไกการจัดการและตอบสนองต่อเหตุการณ์ ในการกำหนดบทบาทและความรับผิดชอบระหว่างลูกค้าและ Tencent Cloud ในกรณีเกิดเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ขั้นตอนในการรายงานเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศที่ตรวจพบโดยผู้ประกอบธุรกิจ • มีการรายงานการติดตามและสถานการณ์ดำเนินการแก้ไขปัญหาที่มีการรายงานโดย ผู้ประกอบธุรกิจ • มีการกำหนดขั้นตอนและเงื่อนไขในการร้องขอหลักฐาน (Digital evidence) หรือข้อมูลที่เกี่ยวข้องอย่างชัดเจน	Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ ได้จัดเตรียมเอกสารกฎหมายออนไลน์ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งเนื้อหาประกอบด้วย: การจัดทำสัญญาจ้างทำภายนอก ความสัมพันธ์และหน้าที่ความรับผิดชอบ การแบ่งงานกัน การแจ้งเหตุการณ์ กลไกการระงับข้อพิพาท และประเด็นความคาดหวังอื่นๆ ของคู่สัญญา นอกจากนี้ลูกค้ายังสามารถเจรจาเพื่อเพิ่มข้อกำหนดพิเศษในสัญญาแยกต่างหากได้ ในด้านการตรวจจับและตอบสนองต่อเหตุการณ์ Tencent Cloud ได้สร้างขั้นตอนการจัดการเหตุการณ์โดยละเอียด โดยใช้ระบบการดำเนินงานความปลอดภัยภายในเพื่อบันทึกเหตุการณ์ความปลอดภัยสำหรับเหตุการณ์ความปลอดภัยที่ตรวจจับและระบุได้ Tencent Cloud จะวิเคราะห์และจำแนกระดับเหตุการณ์โดยพิจารณาจากปัจจัยต่างๆ เช่น ลักษณะของเหตุการณ์ ระดับความอ่อนไหวของข้อมูล และขอบเขตของผลกระทบ และจะแจ้งให้ผู้รับผิดชอบที่เกี่ยวข้องทราบทันทีเพื่อดำเนินการจัดการเหตุการณ์ ทีมงานความปลอดภัยของ Tencent Cloud ใช้ระบบการดำเนินงานความปลอดภัยแบบ 24 ชั่วโมงทุกวัน โดยมุ่งเน้นไปที่สถานการณ์หลัก เช่น การเฝ้าระวังช่องโหว่ การติดตามแหล่งที่มาของการบุกรุก และการปิดกั้นการโจมตี ตอบสนองต่อการแจ้งเตือนความปลอดภัยแบบเรียลไทม์ และจัดทำแผนการติดตามแหล่งที่มาของการโจมตีและการจัดการเหตุการณ์ฉุกเฉินอย่างรวดเร็ว เพื่อยับยั้งการแพร่กระจายของเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้ หลือน้อยที่สุด สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการเหตุการณ์ด้าน ความปลอดภัยข้อมูล โปรดดูเนื้อหาในข้อ "11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ " ในคู่มือนี้
2.2.3	การปฏิบัติตาม กฎหมาย	• ผู้ประกอบธุรกิจควรพิจารณาและประเมินข้อกำหนดทางกฎหมายที่ผู้ให้บริการ Cloud Computing อยู่ภายใต้การบังคับใช้ นอกเหนือจากข้อกำหนดทางกฎหมาย ที่ใช้บังคับผู้ประกอบธุรกิจ • ผู้ประกอบธุรกิจควรมีมาตรการตรวจสอบด้านสิทธิและเงื่อนไขการใช้งานซอฟต์แวร์ (Software license) ก่อนดำเนินการติดตั้งลงบนระบบ Cloud Computing เพื่อป้องกันความเสี่ยงจากการละเมิดเงื่อนไขการใช้งาน	ลูกค้าควรพิจารณาและประเมินข้อกำหนดทางกฎหมายและระเบียบข้อบังคับที่ใช้บังคับกับผู้ให้บริการคลาวด์ และควรดำเนินการมาตรการที่จำเป็นเพื่อตรวจสอบสิทธิการอนุญาตและข้อกำหนดการใช้ซอฟต์แวร์ก่อนการติดตั้งซอฟต์แวร์ใดๆ ลงในระบบคอมพิวเตอร์คลาวด์ Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ ดำเนินธุรกิจอยู่อย่างเคร่งครัด Tencent Cloud ได้จัดเตรียมเอกสารกฎหมายออนไลน์ เช่น Terms of ServiceService Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดข้อกำหนดเกี่ยวกับการปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา รวมถึงความรับผิดชอบในการรักษาความลับอย่างชัดเจน Tencent Cloud ได้สร้างขั้นตอนที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านความปลอดภัย เพื่อควบคุมให้ Tencent Cloud ปฏิบัติตามข้อกำหนดด้านกฎหมาย ระเบียบข้อบังคับ และนโยบาย มาตรฐาน และขั้นตอนด้านความปลอดภัยข้อมูล และรับประกันว่าการดำเนินงานและกระบวนการบำรุงรักษา ด้านความปลอดภัยข้อมูลเป็นไปตามข้อกำหนดด้านความปลอดภัยข้อมูลของ Tencent Cloud ฝ่ายกฎหมายของ Tencent Cloud จะรวบรวมข้อกำหนดการปฏิบัติตามข้อกำหนดและกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้องกับธุรกิจของ Tencent Cloud จัดทำรายการกฎหมายและระเบียบข้อบังคับที่สอดคล้องกันตามผลการรวบรวม และอัปเดตทุกปี ข้อกำหนดทางกฎหมายและระเบียบข้อบังคับที่รวบรวมได้ จะถูกเผยแพร่ไปยังฝ่ายงานที่เกี่ยวข้องที่ต้องปฏิบัติตาม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ข้อกำหนดการปฏิบัติตามข้อกำหนด และรับประกันว่าฝ่ายงานที่เกี่ยวข้องสามารถเข้าถึงและปรี กษาข้อกำหนดเหล่านี้ได้ตลอดเวลา
2.2.4	การติดตามและประเมินผู้ให้บริการ	ผู้ประกอบการควรจัดให้มีการติดตาม ประเมิน และทบทวนคุณภาพของการให้บริการของผู้ให้บริการ Cloud Computing แนวทางปฏิบัติที่ควรพิจารณา •ผู้ประกอบการควรกำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรที่ทำหน้าที่ติดตาม ประเมิน และทบทวน การให้บริการอย่างชัดเจน เพื่อให้มั่นใจถึงการปฏิบัติตามสัญญาการให้บริการ และคุณภาพของบริการ ตลอดจน ความเสี่ยงอันอาจเกิดจากการใช้ บริการ •ผู้ประกอบการควรจัดให้มีกระบวนการ ติดตาม ประเมิน และทบทวนการให้บริการของผู้ให้บริการให้เป็นไปตาม ข้อกำหนดในข้อตกลงระหว่างผู้ให้บริการและผู้ให้บริการ Cloud (Cloud Service Agreement)	ลูกค้าควรกำหนดบทบาทและหน้าที่ความรับผิดชอบของ บุคลากรที่รับผิดชอบในการตรวจสอบ ประเมิน และทบทวนการให้บริการให้ชัดเจน และควรตรวจสอบและประเมินคุณภาพบริการของผู้ให้บริการตามข้อตกลงการให้บริการที่ทำระหว่างผู้ให้บริการคลาวด์และตน บริการคลาวด์ที่ Tencent Cloud มอบให้แก่ลูกค้ามีการส่งมอบตามข้อตกลงระดับการให้บริการ (SLA) ที่ตกลงกันสำหรับแต่ละบริการ ตัวชี้วัดประสิทธิภาพ เกณฑ์การวัด และข้อกำหนดในการรายงานสำหรับบริการแต่ละรายการ กำหนดไว้อย่างชัดเจนใน SLA ของผลิตภัณฑ์แต่ละรายการ และเผยแพร่บนเว็บไซต์อย่างเป็นทางการของ Tencent Cloud Tencent Cloud จะติดตามประสิทธิภาพและความพร้อมใช้งานของบริการ คลาวด์อย่างต่อเนื่อง และให้การตรวจสอบแบบเรียลไทม์แก่ลูกค้าผ่านคอนโซล การจัดการ เพื่อสนับสนุนข้อกำหนดการตรวจสอบบุคคลที่สามของลูกค้า Tencent Cloud จะให้ความร่วมมือตามสถานการณ์จริงและตามข้อตกลง ที่ตกลงกับลูกค้า ในการตรวจสอบความปลอดภัยและการกำกับดูแลของบุคคลที่สามของลูกค้า และจัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบที่ลูกค้าเป็นผู้ริเริ่มอย่างแข็งขัน
2.2.5	การยกเลิกหรือสิ้นสุดการใช้บริการ	•ผู้ประกอบการควรพิจารณาความเสี่ยงที่เกี่ยวข้องในการยกเลิกการใช้บริการระบบประมวลผลร่วมกันผ่านเครือข่าย อย่างรอบด้านเพื่อกำหนดกลยุทธ์และจัดทำแผนการยกเลิกการใช้บริการอย่างเหมาะสม เพื่อป้องกันหรือลดผลกระทบ	ลูกค้าควรประเมินความเสี่ยงที่เกี่ยวข้องกับการยกเลิกการใช้บริการคอมพิวเตอร์คลาวด์อย่างรอบด้าน และจัดทำแผนการยุติการใช้บริการที่เหมาะสมและสมเหตุสมผล เพื่อป้องกันหรือบรรเทาผลกระทบจากความเสียหายเหล่านั้น หากลูกค้าจำเป็นต้องยกเลิกข้อตกลงตามสัญญาเนื่องจากมีการเปลี่ยนแปลงธุรกิจหรือการวางแผนเทคโนโลยีสาร

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		อันอาจเกิดขึ้นจากความเสี่ยง	สแนทช์ในอนาคต ลูกค้าสามารถเลือกทำการสำรองข้อมูลและย้ายข้อมูลแล ะสภาพแวดล้อมการผลิตบนคลาวด์ได้ตลอดเวลา ผลิตภัณฑ์คลาวด์ที่ ตามข้อตกลงการให้บริการระหว่าง Tencent Cloud กับลูกค้า หากบริการคลาวด์หมดอายุหรือสิ้นสุดลง สำหรับข้อมูลที่ลูกค้าเก็บไว้ในเซิร์ฟเวอร์คลาวด์เนื่องจาก การใช้บริการ Tencent Cloud ลูกค้าจำเป็นต้องทำการย้ายข้อมูลให้เสร็จสิ้นก่อนช่วงเวลา กักเก็บข้อมูลสิ้นสุดลง Tencent Cloud ให้มารองรับให้ลูกค้าใช้รูปแบบมาตรฐานทั่วไปเพื่อสำรอง และย้ายข้อมูลของลูกค้า และลูกค้าสามารถใช้วิธีการส่งและโปรโตคอลการส่งเดียว กันกับขั้นตอนการย้ายขึ้นคลาวด์ หรือใช้บริการเครือข่าย เช่น Direct Connect (DC) VPN Connection เพื่อให้มั่นใจว่าข้อมูลของลูกค้าในขั้นตอนการย้ายออกจาก คลาวด์มีความปลอดภัยและเชื่อถือได้ เมื่อบริการคลาวด์สิ้นสุดลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยจะลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรอง อย่างสิ้นเชิงหลังจากช่วงเวลากักเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้

13

Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้า
ค้าให้สอดคล้องกับ SEC
หลักเกณฑ์ เงื่อนไข
และวิธีการในการมอบหมายให้
บุคคลอื่น
เป็นผู้รับผิดชอบการในงานที่เกี่ยวข้อง
กับการประกอบธุรกิจ
อย่างไร

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (SEC) ได้ออก [SEC No. Tor Thor 60/2561](#) เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการในการมอบหมายให้บุคคลอื่น

เป็นผู้รับดำเนินการในงานที่เกี่ยวข้องกับการประกอบธุรกิจ

เพื่อชี้แนะผู้ประกอบการธุรกิจบริการหลักทรัพย์ในการใช้มาตรการปฏิบัติที่เหมาะสมเพื่อจัดการความเสี่ยงที่เกี่ยวข้องกับการจ้างบุคคลภายนอกให้ดำเนินการหน้าที่ที่เกี่ยวข้องกับการดำเนินธุรกิจ

และควบคุมและกำกับดูแลการดำเนินงานของบุคคลภายนอกอย่างมีประสิทธิภาพ

ข้อกำหนดหลักครอบคลุมนโยบาย มาตรการ

และขั้นตอนในการมอบหมายหน้าที่การดำเนินงานให้กับบุคคลภายนอก หลักการจ้างบุคคลภายนอก

และเงื่อนไขบังคับสำหรับการจ้างบุคคลภายนอกให้ดำเนินการหน้าที่การดำเนินงาน

ในบทนี้ Tencent Cloud จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จากหลักเกณฑ์ เงื่อนไข และวิธีการในการมอบหมายให้บุคคลอื่น เป็นผู้รับดำเนินการในงานที่เกี่ยวข้องกับการประกอบธุรกิจ และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud จะช่วยผู้ประกอบการธุรกิจบริการหลักทรัพย์ในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

ลำดับ ที่	โดเมนการควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
8	นโยบาย มาตรการ และวิธีปฏิบัติในการมอบหมายให้บุคคลอื่นเป็นผู้รับดำเนินการ	นโยบายในการมอบหมายให้บุคคลอื่นเป็นผู้รับดำเนินการตามข้อต้องระบุรายละเอียดและเป็นไปตามหลักเกณฑ์ดังต่อไปนี้ (1)ขอบเขตและลักษณะงานที่จะให้ดำเนินการ (2)หลักเกณฑ์การคัดเลือกผู้รับดำเนินการซึ่งมีรายละเอียดของแนวทางการพิจารณา ในเรื่องดังนี้ (ก) ฐานะทางการเงิน ซึ่งต้องกำหนดในลักษณะที่จะทำให้สามารถถ่วงน้ำหนักหรือคัดเลือกผู้รับดำเนินการที่ไม่มีความเสี่ยงหรือมีความเสี่ยงทางการเงินที่อาจก่อให้เกิดความเสียหาย หรือมีพฤติกรรมอื่นที่แสดงให้เห็นได้ว่าอยู่ในระหว่างประสบปัญหาทางการเงิน (ข)ความสามารถและความพร้อมในการปฏิบัติงาน ซึ่งต้องกำหนดในลักษณะที่จะทำให้สามารถถ่วงน้ำหนักหรือคัดเลือกผู้รับดำเนินการที่มีระบบงานในการดำเนินการที่เพียงพอและมีประสิทธิภาพ หลายราย	ลูกค้าควรดำเนินการประเมินความเสี่ยงตามระดับความสำคัญของหน้าที่การจ้างทำภายนอก และจัดทำนโยบายการจ้างทำภายนอก กำหนดขอบเขตและลักษณะของหน้าที่การจ้างทำภายนอกให้ชัดเจน กำหนดมาตรฐานการเลือกผู้ให้บริการ และดำเนินการตรวจสอบอย่างละเอียด (due diligence) ต่อผู้ให้บริการตามมาตรฐาน เนื้อหาการตรวจสอบอย่างละเอียดรวมถึง แต่ไม่จำกัดเพียง: สภาพทางการเงิน ความสามารถในการดำเนินงาน ความรู้ความเชี่ยวชาญเฉพาะทาง ชื่อเสียงทางธุรกิจ การให้บริการข้ามพรมแดน ความปลอดภัยข้อมูล การจัดการผู้รับช่วงงาน ฯลฯ Tencent Cloud ได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบอย่างละเอียดของลูกค้าอย่างเข้มข้น ต่อไปนี้เป็นภาพรวมของ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ในด้านต่างๆ ของการตรวจสอบอย่างละเอียด: • สภาพทางการเงิน: Tencent Cloud ซึ่งเป็นแบรนด์คอมพิวเตอร์คลาวด์ที่ Tencent Group สร้างขึ้นด้วยความอุตสาหกรรม ได้รับประโยชน์จากความแข็งแกร่งทางการเงินและสภาพทางการเงินที่มั่นคงของ Tencent Group นับตั้งแต่ปี 2010 ที่ Tencent Cloud เริ่มให้บริการคลาวด์แก่สาธารณะอย่างเป็นทางการ

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดความเฉพาะ	การตอบสนองของ Tencent Cloud
	(ค) ความเชี่ยวชาญ ประสบการณ์ และชื่อเสียงในทางธุรกิจ		Tencent Cloud ได้บรรลุแนวโน้มการเติบโตที่โดดเด่นในตัวชี้วัดทางการเงินที่สำคัญ เช่น รายได้และผลกำไร Tencent Cloud ได้รับการยอมรับจากสถาบันวิจัยอุตสาหกรรมระดับโลกชั้นนำ Gartner ติดต่อกันเป็นเวลาสี่ปี โดยอยู่ในอันดับที่สองในด้านมิติด้านกลยุทธ์ในหมวดผู้ผลิตจากประเทศจีน
	(ง) ความพร้อมของผู้รับดำเนินการ ในกรณีที่ได้รับดำเนินการให้ผู้ประกอบธุรกิจ		ประสบการณ์ในการดำเนินงาน: ความสามารถในการดำเนินงานและขนาดของ Tencent Cloud อยู่ในตำแหน่งผู้นำในอุตสาหกรรม ศูนย์ข้อมูลของ Tencent Cloud มีการกระจายตัวอยู่ในหลายภูมิภาคทั่วโลก ครอบคลุมพื้นที่จีนแผ่นดินใหญ่ ภูมิภาคเอเชียแปซิฟิก ภูมิภาคอเมริกาเหนือ และภูมิภาคยุโรป
	(จ) ประวัติการถูกร้องเรียนหรือถูกฟ้องร้องดำเนินคดีในเรื่องที่เกี่ยวข้องกับงาน ที่จะให้ดำเนินการ		ความสามารถทางวิชาชีพและทางเทคนิค: Tencent Cloud ได้แสดงความสามารถทางเทคนิคที่ครอบคลุมในฐานะผู้นำในอุตสาหกรรมผ่านเทคโนโลยีคอมพิวเตอร์คลาวด์ที่แข็งแกร่ง ความสามารถในการประมวลผลข้อมูลขนาดใหญ่ การประยุกต์ใช้ปัญญาประดิษฐ์ การป้องกันความปลอดภัยทางไซเบอร์ เทคโนโลยีคลาวด์เนทีฟ การกระจายตัวของศูนย์ข้อมูลทั่วโลก และโซลูชันอุตสาหกรรม ความสามารถทางเทคนิคเหล่านี้ไม่เพียงรับประกันความมั่นคงและความน่าเชื่อถือของบริการ Tencent Cloud เท่านั้น แต่ยังจัดเตรียมสภาพแวดล้อมคอมพิวเตอร์คลาวด์ที่ปลอดภัยและน่าเชื่อถือให้กับลูกค้าด้วย ความสามารถด้านความปลอดภัยในการดำเนินงานที่ครบถ้วนของ Tencent Cloud ยังสามารถให้การสนับสนุนทางเทคนิครอบนาฬิกาสำหรับผลิตภัณฑ์คลาวด์แก่ลูกค้าได้
	(ฉ) ความเกี่ยวข้องกับการบริหารหรือผู้บริหารของผู้ประกอบธุรกิจ		
	(ช) ในกรณีที่ผู้รับดำเนินการอยู่ในต่างประเทศ ต้องพิจารณาถึงการเปลี่ยนแปลงหรือความไม่แน่นอนทางเศรษฐกิจการเมือง สังคม และกฎหมายของประเทศของผู้รับดำเนินการ ตลอดจนความซับซ้อนในการบริหารความต่อเนื่องทางธุรกิจที่อยู่ในต่างประเทศของผู้รับดำเนินการด้วย		
	(3) หลักเกณฑ์การทบทวนและการเปลี่ยนตัวผู้รับดำเนินการ ซึ่งครอบคลุมถึงเรื่องดังนี้		
	(4) แนวทางการพิจารณาในกรณีที่ผู้รับดำเนินการจะให้บุคคลอื่นรับดำเนินการช่วง		
	(5) แนวทางการประเมินความเสี่ยงที่เหมาะสมตามระดับความสำคัญของ งานที่ให้ดำเนินการ		
	(6) ระบบรักษาความปลอดภัยของผู้รับดำเนินการในการดูแลรักษาข้อมูลของ ผู้ประกอบธุรกิจและลูกค้า		ชื่อเสียงทางธุรกิจ: ในฐานะแบรนด์คอมพิวเตอร์คลาวด์ภายใต้การนำของ Tencent ซึ่งเป็นบริษัทชั้นนำในอุตสาหกรรมอินเทอร์เน็ตของจีน Tencent Cloud ได้รับการรับรองจากสถาบันอุตสาหกรรมหลายแห่ง

ลำดับ ที่	โดเมนการค วาคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			มอบโซลูชันคอมพิวเตอร์คลาวด์ที่ครอบคลุม และได้ร่วมมือกับพันธมิตรมากกว่า 11,000 ราย เพื่อมอบโซลูชันอุตสาหกรรมมากกว่า 400 รายการให้กับลูกค้าธุรกิจในกว่า 30 อุตสาหกรรม สถานการณ์การให้บริการแก่สถาบันจำนวนมาก: Tencent Cloud ได้ปรับแต่งโซลูชันประเภทต่างๆ ให้เหมาะกับสถาบันหลักทรัพย์หลายแห่ง โดยมีวัตถุประสงค์เพื่อตอบสนองความต้องการทางธุรกิจ ของลูกค้าหลักทรัพย์อย่างยืดหยุ่น ปรับให้เข้ากับวัฒนธรรมและกลยุทธ์องค์กรที่แตกต่างกันใ ตัวอย่างคล่องตัว การจัดการข้อร้องเรียนหรือคดีความ: Tencent Cloud ให้บริการใบงานผ่านคอนโซลบนเว็บไซต์อย่างเป็นทางการ ร สนับสนุนให้ลูกค้ารายงานความขัดข้อง เหตุการณ์ ปัญหา และข้อร้องเรียนที่เกี่ยวข้องกับความปลอดภัย ความพร้อมใช้งาน และการรักษาความลับ ระบบใบงานของ Tencent Cloud จะจัดลำดับความสำคัญให้กับใบงานของลูกค้าผ่านกลไก การตอบสนองตามระดับ เมื่อทีมเทคนิคระดับแรกไม่สามารถแก้ไขได้อย่างมีประสิทธิภาพ ระบบจะเริ่มกระบวนการยกระดับบริการโดยอัตโนมัติ โดยให้ทีมผลิตภัณฑ์หรือทีมเทคนิคเข้ามามีส่วนร่วมและจั ดการร่วมกัน เพื่อให้มั่นใจว่าความต้องการหรือข้อเสนอแนะของลูกค้าไ ด้รับการตอบสนองและจัดการอย่างทันท่วงที ลูกค้ายังสามารถเลือกแผนบริการที่เหมาะสมเพื่อรับการส ับสนุนพิเศษซึ่งประกอบด้วยกลุ่มสนับสนุนเฉพาะ ผู้จัดการบริการเทคนิคเฉพาะ และบริการเพิ่มมูลค่า การจัดการความเสี่ยงข้ามพรมแดน: โครงสร้างพื้นฐานของ Tencent Cloud ครอบคลุมหลายพื้นที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) โดยแต่ละภูมิภาคเป็นพื้นที่ทางภูมิศาสตร์ที่แยกอิสระ และแต่ละโซนความพร้อมใช้งานเป็นโดเมนการบำรุงรักษา และรับมือเหตุขัดข้องที่แยกจากกัน โซนความพร้อมใช้งานแต่ละแห่งถูกแยกทางกายภาพ

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ลูกค้าสามารถวางระบบและจัดเก็บข้อมูลบนภูมิภาคหรือโ ชนความพร้อมใช้งานที่แตกต่างกันได้อย่างอิสระตามควา มต้องการในการขยายธุรกิจและข้อกำหนดด้านความปลอด ภัยของข้อมูล เพื่อรับประกันความต้องการด้านการรับมือเหตุขัดข้องของ ธุรกิจ ภายในปี 2026 Tencent Cloud ได้ดำเนินการติดตั้งศูนย์ข้อมูลสามแห่งในประเทศไทย โดยศูนย์ข้อมูลแต่ละแห่งมีการจัดการด้านไฟฟ้าและเครือ ข่ายที่เป็นอิสระต่อกัน เพื่อรองรับการจำกัดเก็บ ประมวลผล และสำรองข้อมูลของลูกค้าภายในประเทศได้อย่างมีประสิทธิภาพ ความต่อเนื่องทางธุรกิจ: Tencent Cloud ได้รับการรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจแล้ว Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภ ณฑ์และบริการคลาวด์ และจัดทำกลยุทธ์การตอบสนองที่แตกต่างกัน แผนความต่อเนื่องของธุรกิจ และแผนการกู้คืนจากภัยพิบัติตามผลการวิเคราะห์ เพื่อขึ้นนำองค์กรในการกู้คืนทรัพยากรทางธุรกิจที่เกี่ยวข้อง ง Tencent Cloud ได้จัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดยละ เอียดสำหรับผลิตภัณฑ์คลาวด์ และดำเนินการฝึกซ้อมตามแผนกู้คืนจากภัยพิบัตินั้นอย่า งเคร่งครัดตามข้อกำหนดเป็นประจำ เพื่อรับประกันความทันเวลาความเป็นไปได้ของแผนกู้คืน จากภัยพิบัติ การจัดการผู้รับช่วงงาน: Tencent Cloud ได้จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement สำหรับสถานการณ์การประมวลผลโดยผู้รับช่วงงาน ข้อตกลงได้กำหนดข้อกำหนดต่างๆ อย่างชัดเจน เช่น การให้ความยินยอมล่วงหน้าสำหรับการรับช่วงงาน การแจ้งเตือนก่อนการเพิ่มหรือเปลี่ยนผู้รับช่วงงาน หน้าที่ในการปกป้องข้อมูล เป็นต้น

ลำดับ ที่	โดเมนการค วาคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			โดยปราศจากความยินยอมล่วงหน้าจากลูกค้า Tencent Cloud จะไม่รับช่วงงานการดำเนินการประมวลผลใดๆ ที่ดำเนินการแทนลูกค้าตามสัญญา/ข้อตกลง การเปลี่ยนแปลงใดๆ ที่คาดว่าจะเพิ่มหรือเปลี่ยนแปลงผู้รับช่วงงาน Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านช่องทางต่างๆ เช่น อีเมล นอกจากนี้ ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้ ในด้านการจัดการผู้รับช่วงงาน Tencent Cloud ได้สร้างระบบการจัดการความปลอดภัยห่วงโซ่อุปทานที่สมบูรณ โดยผ่านมาตรการต่างๆ เช่น การประเมินและตรวจสอบการอนุญาตเข้าความปลอดภัยของผู้จัดหาที่เข้มงวด การตรวจสอบและประเมินเป็นประจำ และข้อตกลงการบริการรับช่วงงานที่ชัดเจน เพื่อควบคุมผู้จัดหาได้อย่างมีประสิทธิภาพ และรับประกันว่าการรับช่วงงานจะไม่ส่งผลกระทบต่อความสามารถของ Tencent Cloud ในการให้บริการที่เกี่ยวข้องแก่ลูกค้า ความเป็นความลับและความสมบูรณ์ของกระบวนการประมวลผลข้อมูลลูกค้า ตลอดจนสิทธิในการกำกับดูแลและตรวจสอบของหน่วยงานกำกับดูแลทางการเงินและสถาบันการเงินของประเทศไทย นอกจากนี้ Tencent Cloud จะให้ความร่วมมืออย่างแข็งขันกับข้อกำหนดการจัดการรับช่วงงานของลูกค้า ตอบสนองและสนับสนุนกิจกรรมการตรวจสอบหรือการประเมินที่ลูกค้าเป็นผู้ริเริ่ม เป็นต้น • ความปลอดภัยข้อมูล: เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูล ซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยข้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดการความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ รวมถึงขึ้นการทำงานประจำวันและกระบวนการจัดการของหน่วยงานและพนักงานทุกหน่วยในบริษัท นโยบายความปลอดภัยข้อมูลของ Tencent Cloud

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัยบนคลาวด์สอดคล้องกับนโยบายความปลอดภัยมาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบายความปลอดภัยข้อมูล Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด เพื่อสนับสนุนข้อกำหนดการตรวจสอบบุคคลที่สามของลูกค้า Tencent Cloud จะให้ความร่วมมือตามสถานการณ์จริงและตามข้อตกลงที่ตกลงกับลูกค้า ในการตรวจสอบความปลอดภัยและการกำกับดูแลของบุคคลที่สามของลูกค้า และจัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบที่ลูกค้าเป็นผู้ริเริ่มอย่างแข็งขัน
14	การมอบหมายงานที่มีไซงานที่มีผู้ให้บริการแบบรวมศูนย์	ในการมอบหมายงานที่มีไซงานที่มีผู้ให้บริการแบบรวมศูนย์ให้ผู้ประกอบธุรกิจ พิจารณาคัดเลือกผู้รับดำเนินการที่มีคุณสมบัติและไม่มีลักษณะต้องห้ามดังต่อไปนี้ (1) มีความพร้อมในด้านบุคลากรและระบบงานในการดำเนินงานอย่างเพียงพอ ที่จะทำให้งานของผู้ประกอบธุรกิจเป็นไปตามหลักเกณฑ์การปฏิบัติงานที่คณะกรรมการ ก.ล.ต. คณะกรรมการกำกับตลาดทุน หรือสำนักงาน กำหนดเกี่ยวกับงานที่รับดำเนินการ รวมทั้งระเบียบวิธีปฏิบัติที่ผู้ประกอบธุรกิจกำหนดขึ้นเพื่อให้เป็นไปตามหลักเกณฑ์ดังกล่าว โดยต้องมีระบบที่เพียงพอและมีประสิทธิภาพอย่างน้อยดังต่อไปนี้	ลูกค้าที่จ้างทำภายนอกธุรกิจที่ไม่ใช่แกนกลาง ควรให้มั่นใจว่าผู้ให้บริการมีกลไกการจัดการความเสี่ยง การควบคุมภายใน ความปลอดภัยข้อมูล และการจัดการเหตุการณ์ที่เพียงพอ และควรให้มั่นใจว่าสภาพทางการเงินของผู้ให้บริการมีความเพียงพอ Tencent Cloud ได้จัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบอย่างละเอียดของลูกค้าอย่างแข็งขัน ต่อไปนี้เป็นภาพรวมของ Tencent Cloud ในฐานะผู้ให้บริการคลาวด์ในด้านต่างๆ ของการตรวจสอบอย่างละเอียด: • การจัดการความเสี่ยง: Tencent Cloud ได้กำหนดกรอบการกำกับดูแลความเสี่ยงและขั้นตอนที่เกี่ยวข้อง และปรับปรุงมาตรการจัดการความเสี่ยงและระบบตรวจสอบภายในอย่างต่อเนื่อง โดยการเสริมสร้างวัฒนธรรมความเสี่ยงอย่างต่อเนื่อง Tencent Cloud ปรับปรุงความสามารถในการจัดการความเสี่ยงภายในอย่าง

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดความเฉพาะ	การตอบสนองของ Tencent Cloud
		(ก) ระบบการบริหารความเสี่ยง	มีประสิทธิภาพ
		(ข) ระบบการควบคุมภายใน	และรับประกันการพัฒนาทางธุรกิจที่ยั่งยืนและมีสุขภาพดี
		(ค)ระบบการรักษาความปลอดภัยของข้อมูลเพื่อป้องกันมิให้บุคคลที่ไม่อำนาจ หน้าที่เกี่ยวข้อง ล้วงรู้ หรือแก้ไขเปลี่ยนแปลงข้อมูล รวมทั้งเพื่อป้องกันการล้วงรู้ข้อมูล อันมิพึงเปิดเผย ระหว่างหน่วยงานและบุคลากร	• การจัดการควบคุมภายใน: ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยภายในอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบการจัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามข้อกำหนดและกฎระเบียบ รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็นอิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง
		(ง)ระบบการรองรับเหตุฉุกเฉินในกรณีต่าง ๆ ซึ่งมีการกำหนดขั้นตอนและ ผู้รับผิดชอบในแต่ละกรณีไว้อย่างชัดเจน	• ความปลอดภัยข้อมูล: เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูล ซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยข้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดการความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ รวมถึงชี้้นำการทำงานประจำวันและกระบวนการจัดการของหน่วยงานและพนักงานทุกหน่วยในบริษัท นโยบายความปลอดภัยข้อมูลของ Tencent Cloud จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัย
		(2)ไม่มีเหตุอันควรเชื่อได้ว่ามีฐานะทางการเงินที่อาจก่อให้เกิดความเสียหาย หรือ มีพฤติกรรมอื่นที่แสดงให้เห็นว่า อยู่ระหว่างประสบปัญหาทางการเงิน	
		(3)ไม่มีเหตุอันควรเชื่อได้ว่ามีข้อบกพร่องหรือมีความไม่เหมาะสมเกี่ยวกับ การควบคุมและการปฏิบัติงานอันดีของธุรกิจ	

ลำดับ ที่	โดเมนการค วาคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			บนคลาวด์สอดคล้องกับนโยบายความปลอดภัย มาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบายค วามปลอดภัยข้อมูล Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจ ศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด • ความต่อเนื่องทางธุรกิจ: Tencent Cloud ได้รับการรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจแล้ว Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภั ณฑ์และบริการคลาวด์ และจัดทำกลยุทธ์การตอบสนองที่แตกต่างกัน แผนความต่อเนื่องของธุรกิจ และแผนการกู้คืนจากภัยพิบัติตามผลการวิเคราะห์ เพื่อขึ้นทบทวนการกู้คืนทรัพยากรทางธุรกิจที่เกี่ยวข้อง ง Tencent Cloud ได้จัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดยละ เอียดสำหรับผลิตภัณฑ์คลาวด์ และดำเนินการฝึกซ้อมตามแผนกู้คืนจากภัยพิบัตินั้นอย่าง เคร่งครัดตามข้อกำหนดเป็นประจำ เพื่อรับประกันความทันเวลาความเป็นไปได้ของแผนกู้คืน จากภัยพิบัติ • สภาพทางการเงิน: Tencent Cloud ซึ่งเป็นแบรนด์คอมพิวเตอร์คลาวด์ที่ Tencent Group สร้างขึ้นด้วยความอุตสาหกรรม ได้รับประโยชน์จากความแข็งแกร่งทางการเงินและสภาพ ทางการเงินที่มั่นคงของ Tencent Group นับตั้งแต่ปี 2010 ที่ Tencent Cloud เริ่มให้บริการคลาวด์แก่สาธารณะอย่างเป็นทางการ Tencent Cloud ได้บรรลุแนวโน้มการเติบโตที่โดดเด่นในตัวของอุตสาหกรรม ที่สำคัญ เช่น รายได้และผลกำไร Tencent Cloud ได้รับการยอมรับจากสถาบันวิจัยอุตสาหกรรมระดับโลก ชั้นนำ Gartner ติดต่อกันเป็นเวลาสี่ปี โดยอยู่ในอันดับที่สองในด้านมิติด้านกลยุทธ์ในหมวดผู้ ผลิตจากประเทศจีน

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดความเฉพาะ	การตอบสนองของ Tencent Cloud
19	การมอบหมาย งานที่มีใช้งานที่มี ผู้ให้บริการแบบ รวมศูนย์	ในการมอบหมายงานที่มีใช้งานที่ มีผู้ให้บริการแบบรวมศูนย์ ผู้ประกอบการ ต้องกำกับดูแลการมอบหมายงาน อย่างน้อยในเรื่องดังต่อไปนี้ (1) จัดให้มีการติดตามและทบทวน ความเหมาะสมของการดำเนินการ ของผู้รับดำเนินการ เป็นประจำ โดยอย่างน้อยต้องทบทวนทันทีที่มี เหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อหลักเกณ ท์ที่กำหนดในประกาศนี้ หรือคุณสมบัติหรือลักษณะต้องห ามของผู้รับดำเนินการ ในกรณีที่ปรากฏว่าผู้รับดำเนินการ ขาดคุณสมบัติ มีลักษณะต้องห้าม หรือไม่มี ความเหมาะสมที่จะเป็นผู้รับดำเนิน การอีกต่อไป ต้องเปลี่ยนตัวผู้รับดำเนินการ หรือดำเนินการอื่นใด ตามความเหมาะสมโดยคำนึงถึงพ ลประโยชน์ของลูกค้าเป็นสำคัญเพ ื่อให้ผู้รับดำเนินการปฏิบัติ ให้เป็นไปตามประกาศนี้หรือข้อก หนดที่สำนักงานออกโดยอาศัยอ นาจตามประกาศนี้ (2) จัดทำสรุปการให้บุคคลอื่นเป็น ผู้รับดำเนินการในงานที่เกี่ยวข้อง กับ การประกอบธุรกิจให้ครบถ้วนและ เป็นปัจจุบัน เสนอต่อผู้บริหารที่รับผิดชอบสูงส ุดในการดำเนินงาน ของผู้ประกอบการ (3) จัดเก็บเอกสารหลักฐานที่เกี่ยวข้อง กับการให้บุคคลอื่นเป็นผู้รับ ดำเนินการ ในงานที่เกี่ยวข้องกับการประกอบ ธุรกิจไว้ให้ครบถ้วนและเป็นปัจจุบั น โดยต้องจัดเก็บในลักษณะที่	ลูกค้าที่จ้างทำภายนอกหน้าที่การงานที่ไม่ใช่แกนกลาง ควรเฝ้าระวังและตรวจสอบการดำเนินงานของบริการผู้ให้ บริการเป็นประจำ และรายงานการจ้างทำภายนอกต่อฝ่ายบริหารเป็นประจำ พร้อมเก็บรักษาเอกสารหลักฐานที่เกี่ยวข้องกับหน้าที่การ จ้างทำภายนอกเพื่อความร่วมมือในการให้ความร่วมมือต่อ การตรวจสอบของหน่วยงานกำกับดูแลเมื่อจำเป็น บริการคลาวด์ที่ Tencent Cloud มอบให้แก่ลูกค้ามีการส่งมอบตามข้อตกลงระดับการให้บริ การ (SLA) ที่ตกลงกันสำหรับแต่ละบริการ ตัวชี้วัดประสิทธิภาพ เกณฑ์การวัด และข้อกำหนดในการรายงานสำหรับบริการแต่ละรายการ กำหนดไว้อย่างชัดเจนใน SLA ของผลิตภัณฑ์แต่ละรายการ และเผยแพร่บนเว็บไซต์อย่างเป็นทางการของ Tencent Cloud Tencent Cloud จะติดตามประสิทธิภาพและความพร้อมใช้งานของบริการ คลาวด์อย่างต่อเนื่อง และให้การตรวจสอบแบบเรียลไทม์แก่ลูกค้าผ่านคอนโซล การจัดการ Tencent Cloud จะให้ความร่วมมือตามสถานการณ์จริงและตามข้อตกลง ที่ตกลงกับลูกค้า ในการตรวจสอบความปลอดภัยและการกำกับดูแลของบ คคลที่สามของลูกค้า และจัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและส ับสนุนกิจกรรมการตรวจสอบที่ลูกค้าเป็นผู้ริเริ่มอย่างแข็ง ขัน

ลำดับ ที่	โดเมนการค วาม	ข้อกำหนดความเฉพาะ	การตอบสนองของ Tencent Cloud
		พร้อมให้สำนักงานเรียกดูหรือตรวจ สอบได้โดยไม่ชักช้า	
		(4) จัดให้สำนักงานเข้าตรวจสอบก ารปฏิบัติงานของผู้รับดำเนินการไ ด้ เมื่อสำนักงาน ร้องขอ	
20	เงื่อนไขที่ต้องปฏิบัติในการมอบห มายงาน	ผู้ประกอบการต้องจัดให้มีการทำ สัญญามอบหมายให้บุคคลอื่นเป็น ผู้รับดำเนินการในงานที่เกี่ยวข้อง กับการประกอบธุรกิจเป็นลายลัก ษณอักษร โดยสัญญาดังกล่าว ต้องมีสาระสำคัญอย่างน้อยในเรื่อ ดังต่อไปนี้ (1) หน้าที่และความรับผิดชอบของ ผู้รับดำเนินการ โดยต้องระบุรายละเอียดอย่างน้อย (2) ให้ผู้รับดำเนินการยินยอมให้ สำนักงานเข้าตรวจสอบการปฏิบัติ งาน ของผู้รับดำเนินการ เรียกดู หรือตรวจสอบเอกสารหลักฐานที่เกี่ยวข้องได้ (3) เหตุ เงื่อนไข และวิธีการ ในการเลิกสัญญาหรือระงับการ ดำเนินการ (4) ค่าตอบแทนและค่าใช้จ่ายที่มีก ารเรียกเก็บ ในกรณีที่ผู้รับดำเนินการมอบห มายให้บุคคลอื่นเป็นผู้รับดำเนินการ ช่วง ผู้ประกอบการ ต้องดำเนินการให้ผู้รับดำเนินการ จัดให้มีสัญญาซึ่งมีรายละเอียด ตามที่กำหนดในวรรคหนึ่งด้วย ๗๗ ทั้งนี้ ไม่ว่าจะมีการมอบหมายงานกันก็ ทอดก็ตาม	ลูกค้าควรทำสัญญาเป็นลายลักษณ์อักษรกับผู้ให้บริการ โดยสัญญาควรครอบคลุมอย่างน้อยดังต่อไปนี้: ความรับผิดชอบและหน้าที่ของทั้งสองฝ่าย ข้อกำหนดกรณีฝ่าฝืนสัญญา การจัดการความต่อเนื่องทางธุรกิจ ข้อกำหนดด้านความปลอดภัย การรักษาความลับของข้อมูล สิทธิในการตรวจสอบ ารสิ้นสุดสัญญา ละการจัดการผู้รับช่วงงาน Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสอง ฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้ สำหรับสถานการณ์การประมวลผลโดยผู้รับช่วงงาน ข้อตกลงได้กำหนดข้อกำหนดต่างๆ อย่างชัดเจน เช่น การให้ความยินยอมล่วงหน้าสำหรับการรับช่วงงาน การแจ้งเตือนก่อนการเพิ่มหรือเปลี่ยนผู้รับช่วงงาน หน้าที่ในการปกป้องข้อมูล เป็นต้น โดยปราศจากความยินยอมล่วงหน้าจากลูกค้า Tencent Cloud จะไม่รับช่วงงานการดำเนินการประมวลผลใดๆ ที่ดำเนินการแทนลูกค้าตามสัญญา/ข้อตกลง การเปลี่ยนแปลงใดๆ ที่คาดว่าจะเพิ่มหรือเปลี่ยนแปลงผู้รับช่วงงาน Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านช่องทางต่างๆ เช่น อีเมล นอกจากนี้ ลูกค้ายังสามารถเลือกทำสัญญากับ

ลำดับ ที่	โดเมนการค วาคม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud

Tencent Cloud แบบออฟไลน์

เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้

14

Tencent Cloud

จะปฏิบัติตามและช่วยเหลือลูกค้าให้สอดคล้องกับ OIC
หลักเกณฑ์การกำกับดูแลและ
บริหารจัดการความเสี่ยงด้าน
เทคโนโลยีสารสนเทศ
อย่างไร

สำนักงานคณะกรรมการกำกับดูแลการประกันภัย (OIC) ได้จัดทำ [OIC B.E. 2563 เรื่อง หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของบริษัทประกันชีวิต และ OIC B.E. 2563 เรื่อง](#)

[หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของบริษัทประกันวินาศภัย](#)

เพื่อรับมือกับความเสี่ยงโดยธรรมชาติที่เกิดจากการเปลี่ยนแปลงทางเทคโนโลยีในการดำเนินธุรกิจ เช่น ภัยคุกคามด้านเทคโนโลยีสารสนเทศและไซเบอร์ แม้เป้าหมายการกำกับดูแลจะแตกต่างกัน แต่เนื้อหาของมาตรฐานทั้งสองฉบับเหมือนกันทุกประการ

โดยกำหนดมาตรฐานและขั้นตอนการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เพื่อให้บริษัทประกันภัยสามารถสร้างกลไกการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์ที่เหมาะสมและเป็นระบบ

และดำเนินการตามมาตรฐานสากลในการใช้มาตรการควบคุมที่เหมาะสมเพื่อรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ กำกับดูแลและประเมินแผนปฏิบัติการในการนำเทคโนโลยีสารสนเทศมาใช้

และดำเนินการจัดการการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศและการตรวจสอบเทคโนโลยีสารสนเทศ ข้อกำหนดหลักครอบคลุมการกำกับดูแลและการจัดการความปลอดภัยเทคโนโลยีสารสนเทศ

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ การปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศ

การตรวจสอบเทคโนโลยีสารสนเทศ การกำกับดูแลและการจัดการความปลอดภัยทางไซเบอร์

รวมถึงการรายงานภัยคุกคามทางไซเบอร์หรือภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศ

ในบทนี้ Tencent Cloud จะสรุปและรวบรวมข้อกำหนดควบคุมที่เกี่ยวข้องกับผู้ให้บริการคลาวด์จาก

หลักเกณฑ์การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

และอธิบายโดยละเอียดว่าในฐานะผู้ให้บริการคลาวด์ Tencent Cloud

จะช่วยบริษัทประกันภัยในการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องได้อย่างไร

14.1 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
14	นโยบายความปลอดภัยเทคโนโลยีสารสนเทศ	บริษัทต้องจัดให้มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT security policy) ที่เป็นลายลักษณ์อักษรสอดคล้องกับการนำเทคโนโลยีมาใช้ในการดำเนินธุรกิจและความเสี่ยงที่อาจเกิดขึ้นจากการใช้เทคโนโลยีนั้น โดยนโยบายต้องได้รับการพิจารณาอนุมัติจากคณะกรรมการบริษัท หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย มีการทบทวนอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ และการสื่อสารให้กับบุคลากรของบริษัท	ลูกค้าควรกำหนดและบำรุงรักษานโยบายความปลอดภัยเทคโนโลยีสารสนเทศที่สอดคล้องกับลักษณะ ขนาด และสภาพความเสี่ยงของธุรกิจ ดำเนินการทบทวนและปรับปรุงเป็นประจำ และควรสื่อสารนโยบายดังกล่าวไปยังบุคคลที่เกี่ยวข้องเพื่อการเรียนรู้และการปฏิบัติตาม เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดนโยบายการจัดการความปลอดภัยข้อมูล ซึ่งประกอบด้วยกลยุทธ์โดยรวมด้านความปลอดภัยข้อมูล โครงสร้างองค์กรด้านความปลอดภัย และระบบการจัดการความปลอดภัย เพื่อสนับสนุนการดำเนินงานที่ปลอดภัยและการจัดการความเสี่ยงของแพลตฟอร์มคลาวด์อย่างมีประสิทธิภาพ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ใช้ ทัวท์ซันด์	รวมถึงชี้แจงการทำงานประจำวันและกระบวนการจัดการ ของหน่วยงานและพนักงานทุกหน่วยในบริษัท นโยบายความปลอดภัยข้อมูลของ Tencent Cloud จะถูกทบทวนเป็นระยะ เพื่อกำหนดให้เป้าหมายการควบคุม ขั้นตอนการควบคุม และมาตรการควบคุมของระบบการจัดการความปลอดภัย ภัยบนคลาวด์สอดคล้องกับนโยบายความปลอดภัย มาตรฐาน ขั้นตอน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง และรับประกันความเพียงพอและประสิทธิผลของนโยบาย ความปลอดภัยข้อมูล นอกจากนี้ Tencent Cloud ได้สร้างกรอบการจัดการความเสี่ยงที่ครอบคลุมตามมา ตรฐาน ISO/IEC 27001:2022 และดำเนินกิจกรรมการประเมินความเสี่ยงด้านความปล อดภัยข้อมูลอย่างน้อยปีละหนึ่งครั้ง พนักงานสามารถดูนโยบายเหล่านี้ที่ Tencent Cloud เผยแพร่ผ่านแพลตฟอร์มภายในได้ Tencent Cloud มุ่งมั่นที่จะผนวกการจัดการความปลอดภัยข้อมูลเข้า กับงานจัดการในชีวิตประจำวัน เพื่อให้มั่นใจว่าพนักงานเข้าใจและปฏิบัติตามนโยบายแ ละข้อกำหนดการจัดการความปลอดภัยข้อมูลภายใน นอกจากนี้ Tencent Cloud ยังได้รับใบรับรองและคุณวุฒิด้านความปลอดภัยและการ ปฏิบัติตามข้อกำหนดความเป็นส่วนตัวหลายรายการ เช่น ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301, NIST CSF, SOC ซึ่งพิสูจน์ว่าการจัดการความปลอดภัยและการสร้างการ ป้องกันข้อมูลส่วนบุคคลของ Tencent Cloud เป็นไปตามมาตรฐานการรับรองที่เกี่ยวข้องหรือแนวปฏิบัติ ที่ดีของอุตสาหกรรม และยังได้รับการตรวจสอบจากสถาบันตรวจสอบบุคคล ที่สามมืออาชีพเป็นประจำอีกด้วย
15	การจัดการทรัพยากรมนุษย์	บริษัทต้องมีการบริหารจัดการความม ั่นคงปลอดภัยด้านทรัพยากรบุคคล (human resource security) โดยบุคลากรที่ปฏิบัติงานด้านเทคโนโลยี สารสนเทศ มีหลักเกณฑ์ในการ คัดเลือกเพื่อบรรจุเป็นพนักงาน กฎระเบียบ หรือข้อบังคับระหว่างการปฏิบัติงาน	ลูกค้าควรสร้างกลไกการจัดการทรัพยากรมนุษย์สำหรับ บุคลากรด้านเทคโนโลยีสารสนเทศ โดยก่อนเข้าทำงานควรดำเนินการตรวจสอบประวัติบุคคล ตามมาตรฐานการสรรหาและคัดเลือก กำหนดกฎระเบียบที่พนักงานต้องปฏิบัติตามให้ชัดเจน และควรกำหนดข้อกำหนดด้านความปลอดภัยสำหรับก ารลาออกหรือการเลิกจ้างพนักงาน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการก

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		และการสิ้นสุดการปฏิบัติงาน	กับดูแล Tencent Cloud ได้สร้างมาตรฐานและขั้นตอนการจัดการทรัพยากรบุคคลที่สมบูรณ์ เพื่อให้มั่นใจในการคัดเลือก จ้าง และจัดวางบุคลากรตามข้อกำหนดของตำแหน่งงาน Tencent Cloud ได้สร้างวงจรชีวิตการเข้าทำงานที่ชัดเจน ซึ่งรวมถึงขั้นตอนก่อนเข้าทำงาน ขั้นตอนระหว่างการจ้างงาน และขั้นตอนการลาออก ก่อนเข้าทำงาน ผู้สมัครจะต้องผ่านการสัมภาษณ์ โดย Tencent Cloud จะประเมินว่าตนมีคุณสมบัติตรงตามความสามารถที่ตำแหน่งงานต้องการหรือไม่ ตามกฎหมายที่ใช้บังคับและระดับตำแหน่งงาน ฝ่ายทรัพยากรบุคคลจะทำการตรวจสอบประวัติของผู้สมัครก่อนการจ้างงาน การตรวจสอบประวัติรวมถึงประวัติการทำงานในอดีต การตรวจสอบประวัติอาชญากรรม และการตรวจสอบวุฒิการศึกษา ผลการตรวจสอบประวัติจะถูกบันทึกไว้ในระบบการจัดการทรัพยากรบุคคลของ Tencent Cloud หลังจากรับเข้าทำงาน พนักงานภายในทุกคนต้องลงนามในสัญญาจ้างและข้อตกลงรักษาความลับ โดยสัญญาจ้างได้ระบุกลยุทธ์ความปลอดภัยที่มีอยู่ของ Tencent Cloud รวมถึงความรับผิดชอบด้านความปลอดภัยข้อมูลและความรับผิดชอบในการปกป้องข้อมูลส่วนบุคคลที่พนักงานหรือบุคคลที่สามต้องปฏิบัติตาม ส่วนข้อตกลงรักษาความลับประกอบด้วยข้อผูกพันและความรับผิดชอบในการรักษาความลับของบุคคลที่ลงนาม และบทลงโทษที่อาจได้รับหากมีละเมิดข้อกำหนดในการรักษาความลับ พนักงานภายนอก (Outsourcing) ก็จำเป็นต้องได้รับการตรวจสอบประวัติก่อนการจ้างงาน เช่นเดียวกัน และต้องปฏิบัติตามข้อกำหนดในการรักษาความลับที่กำหนดไว้ในข้อตกลงระหว่าง Tencent Cloud กับผู้ให้บริการภายนอก ข้อกำหนดในการรักษาความลับระหว่าง Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			กับพนักงานและบุคคลที่สามจะได้รับการทบทวนและปรับปรุงโดยฝ่ายกฎหมายตามความจำเป็น ในระหว่างการทำงานของพนักงานหรือบุคคลที่สาม Tencent Cloud ได้สร้างกลไกการฝึกอบรมและการเรียนรู้ด้านความปลอดภัยข้อมูลหลายชุด เพื่อให้ความรู้แก่พนักงานเกี่ยวกับนโยบาย ขั้นตอน และแนวทางปฏิบัติด้านความปลอดภัยข้อมูล พนักงานต้องเข้ารับการฝึกอบรมสร้างจิตสำนึกด้านความปลอดภัยข้อมูลเป็นประจำ ขั้นตอนการลาออกจาก Tencent Cloud รวมถึงการยกเลิกบัญชีผู้ใช้และสิทธิ์การเข้าถึงทันที ตลอดจนกระบวนการเรียกคืนทรัพย์สินของบริษัท เป็นต้น ทรัพย์สินที่มีตัวตนของ Tencent Cloud ถูกจัดสรรให้กับผู้รับผิดชอบที่กำหนดและถูกบันทึกไว้ผ่านระบบติดตามทรัพย์สินเฉพาะภายในของ Tencent Cloud Tencent Cloud จะทำการทบทวนทรัพย์สินเป็นประจำเพื่อยืนยันการมีอยู่จริงของทรัพย์สิน และบันทึกผลการทบทวน
16	การจัดการสินทรัพย์เทคโนโลยีสารสนเทศ	บริษัทต้องจัดให้มีการบริหารจัดการทรัพย์สินสารสนเทศ (asset management) โดยจะต้องมีการดำเนินการอย่างน้อยในเรื่อง ดังต่อไปนี้ (๑) ต้องจัดให้มีการจัดทำทะเบียนรายการทรัพย์สินสารสนเทศ โดยต้องมีการบำรุงรักษาทรัพย์สินสารสนเทศอย่างสม่ำเสมอ รวมถึงต้องจัดให้มีมาตรการด้านความมั่นคงปลอดภัยสำหรับการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์อื่น (๒) ต้องจัดให้มีแนวปฏิบัติการจัดชั้นสารสนเทศ (information classification) ที่เหมาะสมตามชั้นความลับและความสำคัญของสารสนเทศขององค์กร และมีการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยที่สอดคล้องตาม	ลูกค้าควรบำรุงรักษาบัญชีรายการสินทรัพย์ที่ประกอบด้วยสินทรัพย์ข้อมูลทั้งหมด และสร้างกลไกการจัดการสินทรัพย์ข้อมูลเพื่อระบุสินทรัพย์ จัดระดับและหมวดหมู่ กำหนดกรรมสิทธิ์ในสินทรัพย์ และจัดการความปลอดภัยของสินทรัพย์ตามระดับที่แตกต่างกัน บัญชีรายการสินทรัพย์ควรได้รับการทบทวนเป็นประจำ และควรได้รับการปรับปรุงให้ทันสมัยทันทีเมื่อมีการเปลี่ยนแปลง เพื่อช่วยเหลือลูกค้าในการบริหารสินทรัพย์ข้อมูลอย่างครอบคลุม Tencent Cloud Cloud Workload Protection Platform (CWPP) ซึ่งสนับสนุนการรวบรวมลายเซ็นดิจิทัลของสินทรัพย์โดยอัตโนมัติ และบริหารจัดการข้อมูลลายเซ็นดิจิทัลของสินทรัพย์ เช่น บัญชีผู้ใช้ พอร์ต กระบวนการ และแอปพลิเคชัน อย่างเป็นเอกภาพ CWPP ยังสามารถดำเนินการตรวจสอบอย่างรวดเร็วเกี่ยวกับขอบเขตผลกระทบความเสี่ยงของเหตุการณ์ความปลอดภัยที่เกิดขึ้นแล้ว ตามลายเซ็นดิจิทัลของสินทรัพย์ เพื่อช่วยลูกค้ายกระดับความปลอดภัยของเซิร์ฟเวอร์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
	ชั้นความลับ ซึ่งรวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูล ระหว่างการรับส่งข้อมูลผ่านเครือข่าย สื่อสาร การจัดเก็บข้อมูลในระบบงานหรือสื่อ บันทึกข้อมูลต่าง ๆ และการทำลายข้อมูลที่เหมาะสมกับชั้น ความลับ		ลูกค้ายังสามารถใช้แพลตฟอร์มการจัดการความปลอดภัย ภัยแบบครบวงจร <u>Cloud Security Center (CSC)</u> ของ Tencent Cloud เพื่อบริหารจัดการความปลอดภัยของสินทรัพย์ข้อมูล CSC มีฟังก์ชันศูนย์ความปลอดภัยสินทรัพย์ ซึ่งช่วยให้ลูกค้าสามารถตรวจนับสินทรัพย์บนคลาวด์แ บบไดนามิกโดยอัตโนมัติ รวมถึงเซิร์ฟเวอร์คลาวด์ ที่เก็บวัตถุ ฐานข้อมูลคลาวด์ โหลดบาลานเซอร์ เป็นต้น และบริหารจัดการความเสี่ยงด้านความปลอดภัยของสิ นทรัพย์แบบครบวงจรผ่านหลายมิติความปลอดภัย เช่น ความเสี่ยงการกำหนดค่าคลาวด์ ช่องโหว่ และเหตุการณ์ความปลอดภัย เพื่อลดความเสี่ยง "IT ล่องหน" บนคลาวด์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำ กับดูแล ในด้านการจัดการสินทรัพย์ข้อมูล Tencent Cloud ได้กำหนดมาตรฐานการจัดการสินทรัพย์ข้อมูลและกระ บวนการจัดการตลอดวงจรชีวิตสินทรัพย์ เพื่อจัดการและปกป้องสินทรัพย์ เช่น ข้อมูลอิเล็กทรอนิกส์ ฮาร์ดแวร์และอุปกรณ์เสมือน โครงสร้างพื้นฐาน ระบบแอปพลิเคชัน และซอฟต์แวร์ โดยจำแนกประเภทและระดับ Tencent Cloud ใช้ระบบการจัดการสินทรัพย์ในการบริหารจัดการอุปกร ณ์ฮาร์ดแวร์และส่วนประกอบซอฟต์แวร์ รวมถึงการลงทะเบียนและผูกมัดสินทรัพย์ การตรวจนับและการอัปเดตข้อมูลสินทรัพย์ การปลดระวางและเปลี่ยนใหม่สินทรัพย์ เป็นต้น เพื่อรับประกันการทำงานที่ราบรื่นของระบบพื้นฐานของ แพลตฟอร์มคลาวด์ และจัดเตรียมการสนับสนุนที่เชื่อถือได้ให้กับระบบธุรกิจ สำหรับฮาร์ดดิสก์ที่ปลดระวางแล้ว Tencent Cloud ใช้วิธีการทำลายทางกายภาพที่ปลอดภัย เพื่อรับประกันว่าฮาร์ดดิสก์ถูกทำลายอย่างสมบูรณ์ และมีการบันทึกการไถ่ในบันทึกการทำลาย Tencent Cloud ยังได้กำหนดนโยบายการใช้งานที่ยอมรับได้ (Acceptable Use Policy) ซึ่งกำหนดความรับผิดชอบและหน้าที่ของพนักงานและ บุคคลที่สามในการใช้ทรัพยากรของบริษัท Tencent Cloud (รวมถึงระบบเทคโนโลยีสารสนเทศ เครือข่าย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			อุปกรณ์ ข้อมูล ฯลฯ) ควบคุมพฤติกรรมการใช้งานที่เหมาะสม และป้องกันความเสี่ยงที่อาจเกิดขึ้น เพื่อให้แน่ใจในความเป็นความลับและความสมบูรณ์ของ ข้อมูลลูกค้า ในด้านการป้องกันการจัดเก็บข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการ ของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่ง สูง และผสานรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล Key Management Service (KMS) ใช้โมดูลความปลอดภัยฮาร์ดแวร์ (HSM) ที่ได้รับการรับรอง FIPS-140-2 ในการสร้างและปกป้องคีย์ และสามารถสนับสนุนการจัดการวงจรชีวิตเต็มรูปแบบ ของคีย์การเข้ารหัสของลูกค้า ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความ ปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มานั้นก็มีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับ ธุรกิจของลูกค้า นอกจากนี้ ลูกค้ายังสามารถใช้บริการ Direct Connect (DC) และ VPN Connection เพื่อให้บริการถ่ายโอนข้อมูลที่ปลอดภัยในสถานการณ์ ต่างๆ สำหรับการลบและทำลายข้อมูล Tencent Cloud มีกลไกทำลายข้อมูลที่ปลอดภัยและเชื่อถือได้ เมื่อบริการของลูกค้าหมดอายุลง Tencent Cloud ปฏิบัติตามวิธีการลบข้อมูลอย่างเข้มงวด โดยลบข้อมูลลูกค้า รวมถึงสำเนาและข้อมูลสำรอง อย่างสิ้นเชิงหลังช่วงเวลาเก็บข้อมูลสิ้นสุดลง ข้อมูลที่ถูกลบไปแล้วไม่สามารถกู้คืนได้ เมื่อสื่อที่ใช้ให้บริการ Tencent Cloud เกิดความขัดข้องและจำเป็นต้องเปลี่ยนหรือถึงอายุการใ้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ใช้งานและจำเป็นต้องกำจัด Tencent Cloud จะลบข้อมูลที่เหลืออยู่ทันที และปฏิบัติตามขั้นตอนที่เข้มงวดเพื่อทำลายทางกายภาพอย่างสมบูรณ์ในเวลาที่เหมาะสม
17	การควบคุมการเข้าถึง	บริษัทต้องจัดให้มีการควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินสารสนเทศ (access control) เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต โดยจะต้องมีการดำเนินการอย่างน้อยในเรื่อง ดังต่อไปนี้ (๑) กำหนดนโยบายการเข้าถึงหรือใช้งานระบบ ข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศ รวมถึงนโยบายการใช้บริการเครือข่ายสื่อสารขององค์กร สอดคล้องตามข้อกำหนดการดำเนินธุรกิจ (๒) กำหนดให้มีการบริหารจัดการสิทธิการใช้งานและตรวจสอบยืนยันตัวตนตามสิทธิ ที่กำหนดไว้ โดยคำนึงถึงความจำเป็นในการใช้งาน และระดับความเสี่ยง (๓) กำหนดให้มีการทบทวนปรับปรุงสิทธิการใช้งานตามรอบระยะเวลาที่กำหนด (๔) กำหนดให้มีการเพิกถอนสิทธิการใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่งานหรือสิ้นสุด สภาพการเป็นพนักงาน	ลูกค้าควรควบคุมการเข้าถึงระบบ ข้อมูล และทรัพย์สินเทคโนโลยีสารสนเทศ ทำการพิสูจน์ตัวตนผู้ใช้และตรวจสอบสิทธิ์ที่เกี่ยวข้อง ทบทวนและอัปเดตสิทธิการใช้งานของผู้ใช้เป็นประจำ และเพิกถอนสิทธิ์ทันทีเมื่อพนักงานลาออกหรือมีการเปลี่ยนแปลงหน้าที่การงาน ในด้านการจัดการบัญชีผู้ใช้และการให้สิทธิ์ Cloud Access Management (CAM) สามารถช่วยลูกค้าจัดการการเข้าถึงผลิตภัณฑ์และบริการของ Tencent Cloud ได้อย่างปลอดภัยและยืดหยุ่น Tencent Cloud ยังได้กำหนดกลยุทธ์การให้สิทธิ์การควบคุมการเข้าถึงและกลไกเกมทริกซ์การแบ่งแยกสิทธิ์ภายในองค์กร Tencent Cloud ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการตรวจสอบสิทธิ์การเข้าถึงของพนักงาน โดยผู้ใช้ต้องผ่านการยืนยันตัวตนสองปัจจัยก่อนเข้าถึงทรัพยากรภายใน Tencent Cloud ปฏิบัติตามหลักการสิทธิ์น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิ์น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิ์เฉพาะก็ต่อเมื่อมีความจำเป็นต้องใช้ และผ่านกระบวนการอนุมัติสิทธิ์ที่เข้มงวดเท่านั้น Tencent Cloud จะรักษาบันทึกข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดการตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์ สำหรับผู้ที่มีสิทธิ์สูง Tencent Cloud มี Bastion Host (BH) ที่สามารถรองรับการให้สิทธิ์อย่างละเอียดตามมิติต่างๆ เช่น ผู้ใช้ สิทธิ์บัญชี บัญชี และสิทธิ์การดำเนินงาน เพื่อให้มั่นใจว่าสิทธิ์ที่ผู้ใช้มีอยู่เป็นสิทธิ์ขั้นต่ำที่จำเป็นสำหรับการเข้าถึงสิทธิ์และทำงานให้สำเร็จ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
18	เทคโนโลยีการ เข้ารหัส	บริษัทต้องจัดให้มีแนวปฏิบัติด้านการ เข้ารหัสข้อมูล (cryptography) ในการ รักษาความมั่นคงปลอดภัยของข้อมูล ที่เหมาะสมตามชั้นความลับและความ สำคัญของข้อมูลสารสนเทศ	สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้ เครื่องบินคัมกัน อย่างเต็มรูปแบบ โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบ แบ็กเอนด์จากส่วนกลางผ่าน เครื่องบินคัมกัน การเข้าถึง เครื่องบินคัมกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติสิทธิ์ มีเฉพาะเจ้าหน้าที่ปฏิบัติการภายในของ Tencent Cloud บางส่วนเท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบ เครื่องบินคัมกัน ต้องการการยืนยันตัวตนสองปัจจัย บันทึกการดำเนินการปฏิบัติงานแบ็กเอนด์ทั้งหมดจะถูก เก็บไว้โดยศูนย์กลางแพลตฟอร์มบันทึก (log) และได้รับการตรวจสอบโดยทีมตรวจสอบภายในของ Tencent Cloud เป็นประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมการเข้าถึง โปรดดูเนื้อหาในข้อ "3.1, 3.2 การควบคุมการเข้าถึง" ของ "5.3 เอกสารแนบ 2 <u>การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ</u> <u>ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ</u> ในคู่มือนี้
			ลูกค้าควรจำแนกระดับข้อมูลตามความลับและความสำคัญ ของข้อมูล และกำหนดมาตรการเข้ารหัสเพื่อความปลอดภัยของข้อมูล ที่สอดคล้องกันตามระดับข้อมูลที่แตกต่างกัน ในด้านการป้องกันการจัดเก็บข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสานรวม <u>Key Management Service (KMS)</u> เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล ในด้านการป้องกันการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มานั้นก็มีความสามารถด้านความปลอดภัย เช่น

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า ในด้านการจัดการคีย์ Tencent Cloud ยังได้กำหนดมาตรฐานการเข้ารหัสและการจัดการคีย์ โดยกำหนดข้อกำหนดด้านความปลอดภัยสำหรับกระบวนการต่างๆ ในการสมัครคีย์ การสร้าง การจัดเก็บ การใช้ การส่งต่อ การอัปเดต และการทำลายคีย์ การดำเนินการต่างๆ ที่เกี่ยวข้องกับวงจรชีวิตของคีย์ทั้งหมดต้องปฏิบัติตามข้อกำหนดพื้นฐานของการควบคุมสองชั้น การส่งมอบที่เข้มงวด การเก็บรักษาที่เหมาะสม และการอัปเดตที่ทันทั่วทั้ง กระบวนการใช้คีย์ยังต้องแน่ใจว่าปฏิบัติตามข้อกำหนด เช่น การแยกหน้าที่และความรับผิดชอบ การอนุมัติที่เข้มงวด และการดำเนินการด้วยข้อจริง และต้องเก็บรักษาบันทึกการดำเนินการคีย์ทางธุรกิจ และดำเนินการตรวจสอบการดำเนินการเป็นประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการเทคโนโลยีการเข้ารหัส โปรดดูเนื้อหาในข้อ "6 การควบคุมการเข้ารหัส" ของ " 11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ " ในคู่มือนี้
19	ความปลอดภัยทางกายภาพและสิ่งแวดล้อม	บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ของศูนย์คอมพิวเตอร์ สถานที่ปฏิบัติงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และพื้นที่ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศที่สำคัญ โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้ (๑) ต้องจัดให้มีระเบียบปฏิบัติการเข้าถึงศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษร (๒) ต้องจัดให้มีการควบคุมการเข้าและออกศูนย์คอมพิวเตอร์ โดยจำกัดสิทธิการเข้าถึง	ลูกค้าควรใช้มาตรการตรวจสอบและควบคุมการเข้าถึงที่จำเป็นสำหรับศูนย์ข้อมูล เพื่อรับประกันความปลอดภัยทางกายภาพและสิ่งแวดล้อมของศูนย์ข้อมูล โครงสร้างพื้นฐานของ Tencent Cloud มีการกระจายตัวอยู่ในหลายสถานที่ทั่วโลก ประกอบด้วยภูมิภาค (region) และโซนความพร้อมใช้งาน (availability zone) ภูมิภาค (region) แต่ละแห่งเป็นพื้นที่ทางภูมิศาสตร์อิสระ ในขณะที่โซนความพร้อมใช้งานแต่ละโซนเป็นโดเมนการบำรุงรักษาความล้มเหลวอิสระ และแต่ละโซนความพร้อมใช้งานถูกแยกจากกันทางกายภาพ ลูกค้าสามารถปรับใช้ข้อมูลและระบบในภูมิภาคหรือโซนความพร้อมใช้งานที่แตกต่างกันได้อย่างยืดหยุ่นตามคว

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ศูนย์คอมพิวเตอร์ที่เหมาะสม รวมทั้งมีการบันทึกและจัดเก็บข้อมูล การเข้าและออก (๓) ต้องจัดให้มีระบบการป้องกันและกร ะบวนการบำรุงรักษาอุปกรณ์ คอมพิวเตอร์ และ ระบบสาธารณูปโภค (facility) ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น ระบบไฟฟ้าสำรองสำหรับ ศูนย์คอมพิวเตอร์ ระบบทำความเย็น ระบบป้องกันหรือสัญญาณเตือนไฟไหม้ และกล้องวงจรปิด เป็นต้น	ความต้องการในการพัฒนาธุรกิจและข้อกำหนดด้านความ ปลอดภัยของข้อมูล เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติ ทางธุรกิจ ในด้านความปลอดภัยของสภาพแวดล้อมศูนย์ ข้อมูล ศูนย์ข้อมูลทั้งหมดของ Tencent Cloud ทั่วโลกดำเนินการเลือกที่ตั้ง ก่อสร้าง หรือเช่าตามมาตรฐานสากลที่เกี่ยวข้องและข้อกำหนด ความปลอดภัยในห้องเก็บ ทั้งระบบไฟฟ้าและระบบปรับอากาศของแต่ละศูนย์ข้อมูล ออกแบบด้วยความเสถียรสูงและแบบซ้ำซ้อนเต็มรูปแบบ ความล้มเหลวของจุดใดจุดหนึ่งจะไม่ส่งผลกระทบต่อความ ต่อเนื่องของไฟฟ้าและการระบายความร้อนของศูนย์ ข้อมูล แต่ละศูนย์ข้อมูลติดตั้งระบบดับเพลิงครบถ้วน รวมถึงระบบตรวจจับไฟในพื้นที่จุดเฉพาะ ระบบดับเพลิงอัตโนมัติ และอุปกรณ์ดับเพลิงด้วยมือสำหรับใช้ในกรณีฉุกเฉิน ภายในศูนย์ข้อมูลแต่ละแห่งติดตั้งพื้นป้องกันไฟฟ้าสถิต ผู้รับ และรางสายไฟทั้งหมดติดตั้งสายกราวด์เพื่อป้องกันความ เสียหายต่ออุปกรณ์จากไฟฟ้าสถิต ในการควบคุมการเข้าถึงศูนย์ข้อมูล Tencent Cloud ได้กำหนดขั้นตอนการเข้าถึงที่เป็นทางการสำหรับการเ เข้าถึงทางกายภาพของศูนย์ข้อมูล บุคคลที่ต้องการเข้าสู่ศูนย์ข้อมูลต้องแสดงตัวตนและนำ หลักฐานแสดงตัวตนมายื่นต่อเจ้าหน้าที่ปฏิบัติการความ ปลอดภัย ผู้จัดการศูนย์ข้อมูลแต่ละแห่งต้องบันทึกและจัดการการ มอบสิทธิ์ การแก้ไข และการยกเลิกสิทธิ์การเข้าถึงในระบบการเข้าถึงศูนย์ข ้อมูลภายในของตน ผู้จัดการศูนย์ข้อมูลจะทบทวนสิทธิ์การเข้าถึงศูนย์ข้อมูล เป็นประจำ เพื่อให้มั่นใจว่าการจัดสรรสิทธิ์การเข้าถึงอย่างเหมาะสม หากสิทธิ์การเข้าถึงไม่เกี่ยวข้องหรือไม่จำเป็นอีกต่อไป ผู้จัดการศูนย์ข้อมูลของ Tencent Cloud จะปิดการใช้งานสิทธิ์การเข้าถึงดังกล่าว ผู้เยี่ยมชมที่ได้รับอนุมัติให้เข้าสู่ศูนย์ข้อมูลของ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Tencent Cloud ล้วนได้รับการดูแลโดยวิศวกรภาคสนามของ Tencent Cloud ผู้เยี่ยมชมหรือพนักงานทุกประเภทที่เข้าออกศูนย์ข้อมูลต้องได้รับการตรวจสอบตัวตนและตรวจสอบสัมภาระที่พกพา และลงทะเบียนสิ่งของที่นำติดตัวมา ในด้านการตรวจสอบและเฝ้าระวังศูนย์ข้อมูลและการตรวจสอบประจำวัน การจัดการการเฝ้าระวังศูนย์ข้อมูลของ Tencent Cloud ครอบคลุมพื้นที่ภายในห้องเซิร์ฟเวอร์แต่ละแห่ง พื้นที่ส่งมอบงาน จุดเข้าออกพื้นที่ศูนย์ข้อมูล และจุดเข้าออกอาคารต่างๆ ภายในพื้นที่ศูนย์ข้อมูล ซึ่งทั้งหมดติดตั้งระบบแจ้งเตือนการเฝ้าระวังด้วยวิดีโอแบบไม่มีจุดบอด 24 ชั่วโมงตลอด 7 วัน และมีเจ้าหน้าที่รักษาความปลอดภัยประจำการ 24 ชั่วโมงตลอด 7 วัน เจ้าหน้าที่รักษาความปลอดภัยของศูนย์ข้อมูลแต่ละแห่งของ Tencent Cloud ดำเนินการตรวจสอบสถานการณ์ของห้องเซิร์ฟเวอร์และอุปกรณ์ต่างๆ อย่างเคร่งครัดตามรายการตรวจสอบและแผนการตรวจสอบ โดยครอบคลุมพื้นที่ต่างๆ เช่น จุดเข้าออกอาคาร บริเวณรอบอาคาร และภายในอาคาร พร้อมทั้งลงนามจุดตรวจและบันทึกเวลาในการตรวจสอบ ทันทีที่พบความขัดข้องของโครงสร้างพื้นฐานหรือเหตุการณ์ด้านความปลอดภัย จะเริ่มต้นขั้นตอนการตอบสนองเหตุฉุกเฉินของศูนย์ข้อมูลทันที
20	ความปลอดภัยในการสื่อสาร	บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสารของ บริษัท (network and communication security) โดยจะต้องมีการดำเนินการอย่างน้อยดังต่อไปนี้ (๑) ต้องจัดให้มีการจำแนกโซนเครือข่ายสื่อสาร โดยมีการจัดแบ่งเครือข่ายอย่างเหมาะสม และจัดให้มีการควบคุมการเชื่อมต่อจากระบบงานต่าง ๆ มายังระบบงานที่มีความสำคัญอย่างเช่	ลูกค้าควรสร้างกลไกการแยกส่วนเครือข่ายและโดเมนควบคุมสิทธิ์การเข้าถึงระบบเครือข่ายและระบบการเข้าถึงระยะไกล และเสริมสร้างการป้องกันความปลอดภัยของการเชื่อมต่อกับเครือข่ายภายนอก ในด้านการปกป้องการถ่ายโอนข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจก็มีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
	มงวด		เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับ ธุรกิจของลูกค้า Direct Connect (DC) : จัดเตรียมการเชื่อมต่อเครือข่ายแบนด์วิดท์สูงที่มีความ เฉพาะตัวและความปลอดภัยสูง ผู้ใช้เป็นเจ้าของลิงก์เครือข่ายโดยเฉพาะ ไม่มีความเสี่ยงข้อมูลรั่วไหล นอกจากนี้ ลูกค้ายังสามารถใช้ Cloud Connect Network (CCN) เพื่อให้บริการการเชื่อมต่ออินเทอร์เน็ตที่ปลอดภัยระหว่าง Virtual Private Cloud (VPC) บนคลาวด์ และระหว่าง VPC กับศูนย์ข้อมูลในพื้นที่ (IDC)
	(๒)ต้องจัดให้มีการควบคุมและจำกัดสิ ทธิการเข้าถึงระบบเครือข่าย และระบบสารสนเทศ จากระยะไกล (remote access) โดยมีการควบคุมความปลอดภัยในการ เชื่อมต่อระบบเครือข่ายจาก ภายนอก และต้องได้รับการอนุมัติให้มีการเข้าถึง อย่างเหมาะสม		สำหรับข้อกำหนดการแบ่งส่วนเครือข่าย ลูกค้าสามารถใช้บริการ Virtual Private Cloud (VPC) ที่ Tencent Cloud ให้มาเพื่อสร้างพื้นที่เครือข่ายอิสระหลายแห่งสำหรับห พยากรณ์แพลตฟอร์มคลาวด์ที่ได้ซื้อไปแล้ว และกำหนดการแบ่งส่วนเครือข่ายและที่อยู่ IP นโยบายการกำหนดเส้นทาง ฯลฯ ตามต้องการได้ด้วยตนเอง เพื่อดำเนินการป้องกันขอบเขตเครือข่าย Tencent Cloud ให้บริการ EdgeOne (EO) แก่ลูกค้า โดยอิงตามโหนดขอบทั่วโลกของ Tencent Cloud เพื่อมอบบริการป้องกันความปลอดภัยและเร่งความเร็วใ ห้กับลูกค้า มีฟังก์ชัน เช่น การป้องกัน DDoS การป้องกันเว็บฉ้อโกง การป้องกันการโจมตีประเภทบอท/ครอว์เลอร์ การแก้ไข DNS และสนับสนุนให้ลูกค้าสามารถกำหนดกฎการควบคุมก การเข้าถึงแบบกำหนดเองตามความต้องการทางธุรกิจ Cloud Firewall (CFW) ให้การป้องกันขอบเขตเครือข่ายที่แตกต่างกันแก่ลูกค้า เป็นหลัก สนับสนุนการควบคุม ACL ของไฟร์วอลล์อย่างเข้มข้น การปิดกั้น IPS แบบเรียลไทม์ การปะชูดเสมือน และการตรวจจับโค้ดที่เป็นอันตราย ฯลฯ สามารถตอบสนองความต้องการของโซน DMZ ในเครือข่ายแบบดั้งเดิม ปกป้องสินทรัพย์หลักเป็นพิเศษ และบรรลุนโยบายการแยกอย่างละเอียดระหว่าง VPC Web Application Firewall (WAF)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สามารถจัดการกับปัญหาความปลอดภัยของเว็บไซต์และ ละเมิดเว็บไซต์ เช่น การโจมตีเว็บไซต์ การบุกรุก การใช้ประโยชน์จากช่องโหว่ การฝังมัลแวร์ การเปลี่ยนแปลงโดยไม่ได้รับอนุญาต แฮกเกอร์ ครอว์เลอร์ ฯลฯ Anti-DDoS ใช้ทรัพยากรป้องกัน DDoS ที่มีคุณภาพและเพียงพอ ร่วมกับอัลกอริธึมการทำความสะอาดที่พัฒนาอย่างต่อเนื่อง "การพัฒนาด้วยตนเอง + การระบุอัจฉริยะด้วย AI" เพื่อจัดการกับปัญหาการโจมตี DDoS สำหรับการแยกหลายผู้เช่า (Multi-tenancy Isolation) Tencent Cloud มีกลไกความปลอดภัย เช่น นโยบายการควบคุมการเข้าถึงทรัพยากรในชั้นควบคุมแ สมิออน (Virtualization Control Layer) นโยบายการแยกระหว่างเครือข่ายส่วนตัวภายในแพลตฟอร์มคลาวด์ การจัดสรรสิทธิ์และการยืนยันตัวตนบนเว็บคอนโซล รหัสเซสชันของอินเทอร์เน็ตเฟส และคีย์การเข้าถึง เพื่อให้มั่นใจว่าผู้ใช้แต่ละคนสามารถเข้าถึงทรัพยากรค อมพิวเตอร์คลาวด์ที่ตนซื้อได้เท่านั้น ซึ่งทำให้เกิดการแยกการเข้าถึงระหว่างผู้เช่าหลายรายใ ตัวอย่างมีประสิทธิภาพ ในด้านการจัดการควบคุมความปลอดภัยเครือข าย Tencent Cloud ได้ปรับใช้สถาปัตยกรรมความปลอดภัยเครือข่ายที่ครบ ถ้วน โดยใช้กลไกการป้องกันหลายชั้น เช่น ไฟร์วอลล์ ระบบตรวจจับ/ป้องกันการบุกรุก (IDS/IPS) การป้องกัน DDoS การแยกทางตรรกะของเครือข่าย และความปลอดภัยของแอปพลิเคชันเว็บ เพื่อตรวจจับ กรอง และบล็อกการรับส่งข้อมูลเครือข่ายที่เป็นอันตรายได้ทัน ทางที่ ปกป้องความปลอดภัยเครือข่ายของ Tencent Cloud Tencent Cloud ยังติดตั้งระบบตรวจสอบเครือข่ายภายในเพื่อตรวจสอบ และแจ้งเตือนอุปกรณ์เครือข่าย เช่น เราเตอร์ ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย นอกจากนี้ Tencent Cloud ใช้มาตรการต่างๆ เช่น การควบคุมสิทธิ์และขั้นตอนการอนุมัติ เพื่อห้ามไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงทรัพยากร เครือข่ายภายใน ซึ่งรวมถึงเครื่องมือวิเคราะห์และตรวจสอบเครือข่าย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความปลอดภัยในการสื่อสาร โปรดดูเนื้อหาในข้อ "5 การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร" ของ "5.3 เอกสารแนบ 2 การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้
21	ความปลอดภัยในการดำเนินงาน	บริษัทต้องจัดให้มีการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operations security) โดยจะต้องมีการบริหารจัดการและดำเนินการอย่างน้อย ดังต่อไปนี้ (๑)จัดให้มีการบริหารจัดการการเปลี่ยนแปลง (change management) และอนุมัติ การเปลี่ยนแปลงทุกครั้งอย่างเป็นลายลักษณ์อักษร (๒)จัดให้มีการบริหารจัดการขีดความสามารถของระบบ (capacity management) ให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และวางแผนการจัดการให้รองรับการดำเนินงานในอนาคต ได้อย่างมีประสิทธิภาพ (๓)จัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) โดยการบริหาร จัดการการตั้งค่าระบบ (system configuration management) การบริหารจัดการ patch (patch management) การกำหนดสิทธิการเข้าถึงและจำกัดสิทธิการใช้งานของผู้ใช้งานที่มีสิทธิสูง (high privileged ID) (๔)กำหนดวิธีการและกระบวนการที่ใช้ในการสำรองข้อมูล (data backup) รวมทั้ง	ลูกค้าควรสร้างกลไกต่างๆ เช่น การจัดการการเปลี่ยนแปลง การจัดการความจุ การจัดการการกำหนดค่าระบบ การจัดการแพตช์ การจัดการการสำรองข้อมูล การจัดการบันทึก การจัดการการตรวจสอบความปลอดภัย การจัดการช่องโหว่ และการจัดการการทดสอบเจาะระบบ เพื่อรักษาความปลอดภัยในการดำเนินงานของระบบเทคโนโลยีสารสนเทศ ในด้านการจัดการการเปลี่ยนแปลง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานการจัดการสำหรับการเปลี่ยนแปลงผลิตภัณฑ์และการกำหนดค่าที่กำหนดขั้นตอนต่างๆ ในกระบวนการเปลี่ยนแปลงและผู้รับผิดชอบที่เกี่ยวข้องอย่างชัดเจน เพื่อให้มั่นใจว่าการเปลี่ยนแปลงได้รับการอนุมัติและทดสอบอย่างเหมาะสมก่อนการดำเนินการ ในเวลาเดียวกัน Tencent Cloud ได้กำหนดขั้นตอนการจัดการสำหรับการเปลี่ยนแปลงฉุกเฉิน โดยการเปลี่ยนแปลงฉุกเฉินต้องได้รับการอนุมัติที่เหมาะสมก่อนจึงจะสามารถดำเนินการได้ การเปลี่ยนแปลงโปรแกรมทุกประเภท รวมถึงการเปลี่ยนแปลงแอปพลิเคชันและไฟล์กำหนดค่า ระบบปฏิบัติการ และฐานข้อมูล ต้องได้รับการวิเคราะห์ผลกระทบทางธุรกิจก่อนการเปิดตัว จัดทำแผนย้อนกลับสำหรับการเปลี่ยนแปลง และได้รับการอนุมัติจากผู้รับผิดชอบที่เกี่ยวข้อง ระบบเผยแพร่การเปลี่ยนแปลงของ Tencent Cloud บังคับให้การดำเนินการเปลี่ยนแปลงสามารถดำเนินการได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น และเก็บรักษาบันทึกที่เกี่ยวข้องกับการเปลี่ยนแปลงไว้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ความถี่ในการสำรองข้อมูลที่เหมาะสมกับลักษณะและความซับซ้อนของการดำเนินงานของบริษัท (๕) จัดให้มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (logging) ของเครื่องแม่ข่าย ระบบงาน และ อุปกรณ์เครือข่ายที่สำคัญ โดยจะต้องมีความมั่นคงปลอดภัยเพียงพอในการป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย รวมถึงมีการสอบทาน log ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ (๖) จัดให้มีการติดตามดูแลระบบและการเฝ้าระวังภัยคุกคาม (security monitoring) โดยมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติ หรือภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของระบบที่สำคัญ รวมถึงต้องมีการบริหารจัดการช่องโหว่ (vulnerability management) ของระบบที่เหมาะสมตามระดับความเสี่ยง และจัดให้มีผู้เชี่ยวชาญจากภายนอก ทำหน้าที่ทดสอบเจาะระบบ โดยเฉพาะระบบงาน (application) และระบบเครือข่าย (network) ที่มีการเชื่อมต่อกับระบบเครือข่ายสื่อสารสาธารณะ (internet facing) อย่างสม่ำเสมอ หรือทุกครั้ง ที่มีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ	พร้อมทั้งตรวจสอบบันทึกเป็นประจำ หลังการเผยแพร่การเปลี่ยนแปลง Tencent Cloud จะตรวจสอบ ตรวจสอบ และบันทึกผลการเปลี่ยนแปลงในสภาพแวดล้อมการผลิต Tencent Cloud จะจำแนกระดับผลกระทบตามคุณลักษณะของคำขอการดำเนินงานและบำรุงรักษา เช่น ระดับความสำคัญ/เร่งด่วน และขอบเขตของการเปลี่ยนแปลง สำหรับคำขอเปลี่ยนแปลงที่อาจส่งผลกระทบต่อสภาพแวดล้อมภายนอก เช่น ผลิตภัณฑ์ โครงสร้างพื้นฐาน และการกำหนดค่าการขยาย Tencent Cloud จะแจ้งให้ลูกค้าทราบผ่านการประกาศ อีเมล คอนโซลเว็บไซต์อย่างเป็นทางการของ Tencent Cloud และ/หรือช่องทางอื่นที่เหมาะสม สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการเปลี่ยนแปลง โปรดดูเนื้อหาในข้อ "8.2 การบริหารจัดการการเปลี่ยนแปลง" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้ ในด้านการจัดการความจุ เพื่อให้บรรลุการตรวจสอบและจัดการประสิทธิภาพของระบบ ลูกค้าสามารถใช้ Tencent Cloud Observability Platform (TCOP) ซึ่งให้บริการตรวจสอบแบบเรียลไทม์ การวิเคราะห์ และการแจ้งเตือนสำหรับผลิตภัณฑ์/ทรัพยากรคลาวด์ รวบรวมและแสดงตัวชี้วัดการตรวจสอบต่างๆ ที่รายงานโดยผลิตภัณฑ์คลาวด์ เช่น เซิร์ฟเวอร์คลาวด์และฐานข้อมูลคลาวด์ รวมถึงตัวชี้วัดการตรวจสอบที่กำหนดเองและรายงานโดยลูกค้าผ่านแผนภูมิที่มองเห็นได้ ช่วยให้ลูกค้าติดตามอัตราการใช้ทรัพยากรผลิตภัณฑ์คลาวด์ ประสิทธิภาพของแอปพลิเคชัน และสถานะการทำงานของผลิตภัณฑ์คลาวด์แบบเรียลไทม์ และสนับสนุนการตั้งค่าการแจ้งเตือนตามตัวชี้วัด โดยแจ้งให้ลูกค้าทราบถึงความผิดปกติของธุรกิจอย่างทันทางที่ผ่านการส่งข้อความและช่องทางอื่นๆ ตามกฎการแจ้งเตือนที่ตั้งไว้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			Tencent Cloud ทำการคาดการณ์ความต้องการด้านความจุตามความต้องการในการดำเนินงานทางธุรกิจ และจัดทำแผนการจัดการความจุประจำปี โดยใช้แพลตฟอร์มตรวจสอบความจุภายในเพื่อให้เจ้าหน้าที่จัดการความจุเฝ้าติดตามสถานการณ์การใช้ความจุ และตรวจสอบการใช้งานความจุแบบเรียลไทม์ และระบุแนวโน้มการใช้ความจุ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการความจุ โปรดดูเนื้อหาในข้อ "8.3 การบริหารจัดการขีดความสามารถของระบบ" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้ ในด้านการจัดการการกำหนดค่า Cloud Security Center (CSC) ให้ฟังก์ชันการตรวจสอบและประเมินความเสี่ยงการกำหนดค่าผลิตภัณฑ์คลาวด์โดยอัตโนมัติ ช่วยลูกค้าลดความเสี่ยงด้านความปลอดภัยที่เกิดจากข้อผิดพลาดในการกำหนดค่าความปลอดภัยในการใช้ผลิตภัณฑ์คลาวด์ และยกระดับความปลอดภัยโดยรวมบนคลาวด์ ในเวลาเดียวกัน ลูกค้าสามารถใช้ Config เพื่อดำเนินการตรวจสอบและควบคุมทรัพยากรคลาวด์จากส่วนกลาง บันทึกข้อมูลการกำหนดค่าและการเปลี่ยนแปลงการกำหนดค่าของทรัพยากรคลาวด์ต่างๆ ในภูมิภาคต่างๆ ภายใต้อุปกรณ์ของลูกค้าอย่างต่อเนื่อง และอิงตามกฎข้อปฏิบัติที่ดีที่สุดและเทมเพลตแพ็คเกจการปฏิบัติตามข้อกำหนดของ Tencent Cloud เพื่อประเมินความสอดคล้องของการกำหนดค่าทรัพยากรคลาวด์ภายใต้อุปกรณ์อย่างต่อเนื่องโดยอัตโนมัติ และระบุการกำหนดค่าทรัพยากรที่ไม่สอดคล้อง เพื่อให้บรรลุการตรวจสอบและจัดการทรัพยากรคลาวด์โดยอัตโนมัติ เพื่อให้สอดคล้องกับข้อกำหนดการกำกับดูแลของลูกค้า Tencent Cloud ได้กำหนดมาตรฐานการกำหนดค่าความปลอดภัยเครือข่ายและมาตรฐานเส้นฐานความปลอดภัยขึ้น เพื่อจัดการมาตรฐานการกำหนดค่าความปลอดภัยของอุปกรณ์เครือข่าย ไฟร์วอลล์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ระบบปฏิบัติการของเซิร์ฟเวอร์โฮสต์ ฐานข้อมูล และระบบแอปพลิเคชัน Tencent Cloud ใช้เครื่องมือสแกนเพื่อตรวจจับความเบี่ยงเบนของการกำหนดค่าระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และอิมเมจเสมือน (Virtual Image) จากมาตรฐานอย่างต่อเนื่อง สำหรับความเบี่ยงเบนที่ตรวจพบ Tencent Cloud จะสร้างใบงานความปลอดภัยและส่งไปยังทีมงานผู้รับผิดชอบโดยอัตโนมัติ เพื่อดำเนินการแก้ไขทันทีที่ Tencent Cloud ยังทบทวนนโยบายความปลอดภัยและการตั้งค่าพารามิเตอร์ของอุปกรณ์เครือข่าย เช่น เราเตอร์ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย เป็นระยะ เพื่อให้มั่นใจในประสิทธิภาพของนโยบายและพารามิเตอร์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการกำหนดค่า โปรดดูเนื้อหาในข้อ "8.1 การบริหารจัดการการตั้งค่าระบบ" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้ ในด้านการจัดการแพตช์ ลูกค้ายังสามารถใช้ Cloud Workload Protection Platform (CWPP) เพื่อตรวจจับช่องโหว่ซอฟต์แวร์ Linux ช่องโหว่ระบบปฏิบัติการ Windows ช่องโหว่ Web-CMS และช่องโหว่แอปพลิเคชัน แจ้งเตือนแบบเรียลไทม์ และรับโซลูชันการแก้ไขช่องโหว่ ช่วยลูกค้าตอบสนองต่อความเสี่ยงจากช่องโหว่อย่างรวดเร็ว Tencent Container Security Service (TCSS) เป็นระบบแพตช์เสมือนที่ Tencent Cloud Security พัฒนาขึ้นเพื่อป้องกันช่องโหว่วันศูนย์ (zero-day) ที่เกิดขึ้นบ่อยครั้ง ซึ่งผสมผสานเทคโนโลยีการขุดเจาะช่องโหว่และการแจ้งเตือนช่องโหว่ร้ายแรงแบบเรียลไทม์ของ Tencent ใช้เพื่อตรวจจับและวิเคราะห์ช่องโหว่ สร้างแพตช์เสมือนตามความรู้ความเชี่ยวชาญของ Tencent และทำให้แพตช์เสมือนมีผลบนเซิร์ฟเวอร์คลาวด์โดยอัตโนมัติ เพื่อป้องกันการโจมตีของแฮกเกอร์ได้อย่างมีประสิทธิภาพ นอกจากนี้ ลูกค้ายังสามารถใช้ Vulnerability Scanning Service (VSS)

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของอุปกรณ์เครือข่ายและบริการแ อปพลิเคชันขององค์กร และใช้คำแนะนำการแก้ไขที่มีอาชีพจาก VSS เพื่อลดความเสี่ยงด้านความปลอดภัยขององค์กร เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำ กับดูแล ในด้านการจัดการแพตช์ Tencent Cloud จะระบุแพตช์ล่าสุด และดำเนินการทดสอบความปลอดภัยอย่างเพียงพอก่อ นการติดตั้งแพตช์ เพื่อให้มั่นใจในความปลอดภัยของการติดตั้งแพตช์ Tencent Cloud จะแจ้งให้ทีมงานธุรกิจภายในแต่ละทีมทราบเป็นประจำ เกี่ยวกับการอัปเดตและติดตั้งแพตช์ และใช้เครื่องมือตรวจจับจุดปลายทาง (endpoint) สแกนสถานะการติดตั้งแพตช์เป็นประจำ และอุปกรณ์ที่ไม่ได้ติดตั้งแพตช์เกินกำหนดเวลาจะถูก สร้างใบงานแจ้งเตือนโดยอัตโนมัติ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการช่องโหว่และแ พตช์ โปรดดูเนื้อหาในข้อ "8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ๔" ในคู่มือนี้ ในด้านการจัดการการสำรองข้อมูล ในเวลาเดียวกัน Tencent Cloud ได้สร้างหรือเข้าศูนย์ข้อมูลในหลายพื้นที่ทั่วโลกตามมา ตรฐานสากลที่เกี่ยวข้องและข้อกำหนดความปลอดภัยใน ห้องกั้น เพื่อมอบตัวเลือกภูมิภาคและโซนความพร้อมใช้งานหล ายแห่งให้แก่ลูกค้า เพื่อให้เป็นไปตามข้อกำหนดด้านการกู้คืนจากภัยพิบัติ และระดับการบริการของธุรกิจ ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud ให้มา เช่น บริการคอมพิวเตอร์ บริการเครือข่าย บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ ไม่เพียงแต่สามารถจัดเตรียมสถาปัตยกรรมระบบที่มีคว

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ามพร้อมใช้งานสูงให้แก่ลูกค้า แต่ยังสนับสนุนให้ลูกค้ากำหนดกลยุทธ์การสำรองข้อมูล สำหรับระบบและข้อมูลของตนเอง ตอบสนองความต้องการสำรองข้อมูลทุกประเภทของลูกค้า สำหรับข้อมูลของลูกค้าที่จัดเก็บไว้บนคลาวด์ Tencent Cloud ใช้วิธีการสำรองข้อมูลแบบเรียลไทม์ การเก็บข้อมูลสำรองหลายชุด และการสำรองข้อมูลข้ามพื้นที่ เพื่อรับประกันความปลอดภัยและความน่าเชื่อถือของข้อมูลธุรกิจที่ลูกค้าเก็บไว้บนคลาวด์ รวมถึงความพร้อมใช้งานอย่างต่อเนื่อง Tencent Cloud ยังใช้มาตรการป้องกันหลายประการ เช่น ความปลอดภัยทางกายภาพ การควบคุมการเข้าถึง การแยกทางตรรกะ และสนับสนุนให้ลูกค้าใช้ Key Management Service (KMS) และ Cloud Access Management (CAM) เพื่อป้องกันไม่ให้ข้อมูลสำรองของลูกค้าถูกเข้าถึงหรือแก้ไขโดยไม่ได้รับอนุญาต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการสำรองข้อมูล โปรดดูเนื้อหาในข้อ "8.6 การสำรองข้อมูล" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ในคู่มือนี้ ในด้านการจัดการบันทึก Tencent Cloud ให้บริการ Cloud Log Service (CLS) เพื่อช่วยเหลือผู้ใช้ในการแก้ไขปัญหาด้านการดำเนินงาน ธุรกิจ การตรวจสอบความปลอดภัย การตรวจสอบบันทึก และการวิเคราะห์บันทึกผ่านบันทึก Tencent Cloud CLS ใช้การออกแบบสถาปัตยกรรมแบบกระจายที่มีความพร้อมใช้งานสูง จัดเก็บข้อมูลบันทึกด้วยการสำรองข้อมูลหลายชุด ป้องกันไม่ให้ข้อมูลไม่สามารถใช้งานได้เมื่อบริการไหนใดขัดข้อง ให้บริการที่มีความพร้อมใช้งานสูง และรับประกันบริการที่เสถียรและน่าเชื่อถือสำหรับข้อมูลบันทึก ด้วย CloudAudit ผู้ใช้สามารถบันทึกบันทึก ตรวจสอบอย่างต่อเนื่อง และเก็บรักษากิจกรรมบัญชีที่เกี่ยวข้องกับการดำเนินการในโครงสร้างพื้นฐาน Tencent Cloud ทั้งหมด

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ลูกค้าสามารถใช้บริการ Elasticsearch Service (ES) เพื่อรวบรวมและส่งบันทึกแบบเรียลไทม์ของเซิร์ฟเวอร์คลาวด์ คอนเทนเนอร์ และผลิตภัณฑ์คลาวด์อื่นๆ หรือข้อมูลธุรกิจที่มีอยู่และเพิ่มขึ้นของธุรกิจไปยังคลัสเตอร์ ES ของ Tencent Cloud เพื่อจัดเก็บข้อมูลแบบกระจาย และการสืบค้นและการวิเคราะห์ข้อมูล เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้สร้างมาตรฐานและกลไกการรวบรวมและการจัดการบันทึก เพื่อควบคุมการบันทึก การดึงข้อมูล การจัดเก็บ การป้องกัน การวิเคราะห์ และการตรวจสอบบันทึกต่างๆ เช่น บันทึกการเข้าสู่ระบบ บันทึกการดำเนินการ บันทึกระบบทั่วไป และบันทึกเหตุการณ์ความผิดปกติของระบบ เพื่อตรวจจับและป้องกันความผิดปกติและความเสี่ยงของกิจกรรมระบบ บันทึกทั้งหมดถูกรวมเข้าสู่แพลตฟอร์มการจัดการบันทึกของ Tencent Cloud เพื่อการจัดการ และมีการใช้มาตรการสำรองข้อมูลและการป้องกันที่เข้มงวดสำหรับข้อมูลบันทึกที่เกี่ยวข้อง เพื่อป้องกันการแก้ไขและการลบโดยไม่ได้รับอนุญาต Tencent Cloud ดำเนินการตรวจสอบบันทึกผ่านเครื่องมือตรวจสอบอัตโนมัติด้านความปลอดภัยในการปฏิบัติการและทีมตรวจสอบภายใน เพื่อตรวจจับความผิดปกติของระบบหรือการดำเนินการ เพื่อป้องกันความเสี่ยงในการปฏิบัติการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการบันทึก โปรดดูเนื้อหาในข้อ "8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log)" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้ ในด้านการจัดการช่องโหว่และการจัดการการทดสอบเจาะระบบ Tencent Cloud ให้บริการ Penetration Testing Service (PTS) แก่ลูกค้า ด้วยการจำลองเทคนิคการโจมตีและเทคนิคการค้นพบช่องโหว่ที่แฮกเกอร์อาจใช้อย่างเต็มรูปแบบ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ใช้วิธีการและกลไกที่ควบคุมได้และไม่ทำลายล้างเพื่อทำการตรวจสอบความปลอดภัยของระบบเป้าหมายอย่างลึกซึ้ง ค้นหาจุดอ่อนที่มีอยู่ในเป้าหมายและอุปกรณ์เครือข่ายให้คำแนะนำในการเสริมความแข็งแกร่งด้านความปลอดภัยเพื่อช่วยลูกค้ายกระดับความปลอดภัยของระบบและสนับสนุนการตรวจสอบหลังการแก้ไขช่องโหว่ ในด้านการสแกนช่องโหว่ ลูกค้าสามารถเลือกใช้ <u>Vulnerability Scanning Service (VSS)</u> เพื่อตรวจสอบสินทรัพย์เครือข่ายขององค์กรและระบุความเสี่ยงของสินทรัพย์นั้นๆ โดยใช้ประโยชน์จากประสบการณ์ด้านความปลอดภัยและข่าวกรองภัยคุกคามที่สะสมมาหลายปีของ Tencent Cloud VSS ได้สร้างฐานข้อมูลกฎช่องโหว่ที่อุดมสมบูรณ์และครอบคลุม และมีความสามารถในการตรวจจับช่องโหว่ 0Day/1Day/NDay ที่มีอาชีวะและมีประสิทธิภาพสูงสามารถดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของสินทรัพย์ของลูกค้า ให้คำแนะนำการแก้ไขที่มีอาชีวะแก่ลูกค้า เพื่อลดความเสี่ยงด้านความปลอดภัย VSS ยังสนับสนุนการทำงานร่วมกับผลิตภัณฑ์คลาวด์ เช่น ความปลอดภัยโฮสต์ ไฟร์วอลล์แอปพลิเคชันเว็บ เพื่อให้บรรลุวงจรปิดจากการตรวจสอบความเสี่ยงไปจนถึงการจัดการความเสี่ยง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะสร้างงานสแกนเป็นประจำผ่านระบบสแกนช่องโหว่เพื่อสแกนช่องโหว่ของสินทรัพย์ในสภาพแวดล้อมคลาวด์และวีเคราะห์ จัดประเภท และดำเนินการแก้ไขช่องโหว่ที่พบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะดำเนินการทดสอบเจาะระบบขนาดใหญ่แบบเต็มวงจรถือเป็นประจำ และดำเนินการทดสอบเจาะระบบแบบเจาะจงอย่างยืดหยุ่นในสถานการณ์ต่างๆ เช่น ก่อนการเปิดตัวผลิตภัณฑ์ใหม่หรือเมื่อมีการเปลี่ยนแปลงครั้งสำคัญ ผลการทดสอบเจาะระบบจะแจ้งให้ฝ่ายงานผู้รับผิดชอบ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ที่เกี่ยวข้องทราบผ่านในงานความปลอดภัย และฝ่ายงานผู้รับผิดชอบจะดำเนินการปะชองให้หรือ ดำเนินมาตรการควบคุมชดเชยอื่นๆ ทันที เพื่อให้มั่นใจว่าช่องโหว่ที่ไ้ประโยชน์ได้ซึ่งพบในการทดสอบเจาะระบบได้รับการจัดการอย่างเหมาะสม นอกจากนี้ Tencent Cloud ยังดำเนินการฝึกซ้อมการต่อสู้เสมือนระหว่างทีมแดงและทีมน้ำเงินเพื่อจำลองการต้านทานการโจมตีทางเครือข่ายเป็นประจำ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการช่องโหว่และการจัดการการทดสอบเจาะระบบ โปรดดูเนื้อหาในข้อ "8.9 การประเมินช่องโหว่ทางเทคนิค & 8.10 การทดสอบการเจาะระบบ" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้
22	การจัดการและการพัฒนาระบบ	บริษัทต้องมีหลักเกณฑ์และกระบวนการในการจัดหาและการพัฒนาระบบ (system acquisition and development) ดังต่อไปนี้ (๑) ในการจัดหาระบบ (system acquisition) บริษัทต้องมีการกำหนดหลักเกณฑ์ที่ชัดเจนในการประเมินและคัดเลือกผู้ขาย หรือผู้รับจ้างพัฒนาระบบ ซึ่งต้องทำสัญญาซื้อขายหรือสัญญาจ้างที่กำหนดเงื่อนไขในการพัฒนาระบบที่ชัดเจน (๒) ในการพัฒนาระบบ (system development) บริษัทต้องจัดให้มีการออกแบบ พัฒนา และทดสอบระบบ เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ และพร้อมใช้งาน โดยจะต้องมีการดำเนินการอย่างน้อย ดังนี้ (ก) มีการจัดทำเอกสารความต้องการระบบงาน (requirement) และเอกสารรายละเอียดคุณสมบัติทางเทคนิค	ลูกค้าควรสร้างกรอบการจัดการวงจรชีวิตการพัฒนาระบบ โดยรวมข้อกำหนดด้านความปลอดภัยในแต่ละขั้นตอนของวงจรชีวิตการพัฒนาระบบ ลูกค้าสามารถใช้เครื่องมือนักพัฒนา Cloud-Native Build (CNB) ที่ Tencent Cloud ให้มา CNB ผสานแนวคิดการพัฒนารายบุคคล (Agile) อย่างลึกซึ้ง ตั้งแต่ issue การรวมคำขอ ไปจนถึงชุดงาน กระบวนการพัฒนารายบุคคลได้รับการจัดตั้งขึ้นอย่างเป็นระเบียบ ช่วยลูกค้ายืนยันผลลัพธ์ของการเปิดตัวเวอร์ชันผลิตภัณฑ์สู่ตลาดด้วยงบประมาณที่ต่ำลงและวิธีการวนซ้ำที่เร็วขึ้น ในด้านการจัดการวงจรชีวิตการพัฒนาระบบความปลอดภัย Tencent Cloud ยังได้สร้างมาตรฐานการพัฒนาระบบความปลอดภัยระบบสารสนเทศภายในองค์กร และมุ่งมั่นผสานมาตรฐาน ISO/IEC 20000 การจัดการบริการเทคโนโลยีสารสนเทศ ระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001 และมาตรฐานระบบการจัดการคุณภาพ ISO/IEC 9001 เข้ากับกระบวนการวงจรชีวิตการพัฒนาระบบความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		(technical specification) โดยครอบคลุมถึงเรื่องการรักษาความ มั่นคงปลอดภัย ซึ่งรวมถึงกระบวนการในการทดสอบประ บบงาน (ข) มีกระบวนการหรือเครื่องมือในการ ควบคุมเวอร์ชันของคำสั่งในการเขียนโ โปรแกรม (source code version control) โดยจะต้องจำกัดสิทธิผู้ที่ดำเนินการ ติดตั้งโปรแกรมในระบบงาน ที่ให้บริการจริง (production) เท่าที่จำเป็น (ค) มีการแบ่งแยกบทบาทหน้าที่และคว ามรับผิดชอบของผู้ที่เกี่ยวข้องใน กระบวนการพัฒนาระบบ เช่น การแบ่งแยกระหว่างผู้พัฒนาระบบ (developer) และผู้บริหารจัดการน ระบบ (administrator) (ง) มีการแบ่งแยกสภาพแวดล้อมของระ บบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากกระบวนการให้บริการจริง (production) (จ) มีการทดสอบระบบก่อนการใช้งาน จริง เช่น ทดสอบการทำงานของแต่ละระบบ (unit test) ทดสอบการทำงานร่วมกันของระบบต าง ๆ (system integration test) ทดสอบความพร้อม ใช้งานตามกระบวนการและความต้อง การของผู้ใช้งาน (user acceptance test) และทดสอบม ความปลอดภัยของระบบ (security test) ตามกระบวนการในการรักษาความมั่น คงปลอดภัยที่กำหนด ในเอกสารรายละเอียดคุณสมบัติทาง	ผลิตภัณฑ์ทั้งหมด ให้มีความสำคัญกับขั้นตอนต่างๆ เช่น ความต้องการ การออกแบบ การวิจัยและพัฒนา การทดสอบ การส่งมอบ และการดำเนินการและบำรุงรักษา พยานแนวคิดด้านความปลอดภัยข้อมูลและการปกป้อง ความเป็นส่วนตัวเข้าไปในแต่ละขั้นตอนของการพัฒนา ผลิตภัณฑ์ เพื่อให้มั่นใจว่าผลิตภัณฑ์คลาวด์ได้รับความควบคุมด้ว ความปลอดภัยที่เพียงพอตลอดวงจรชีวิตของผลิตภั ณฑ์ มาตรการควบคุมความปลอดภัยที่เกี่ยวข้อง ได้แก่: • การฝึกอบรมความปลอดภัย: ส่งเสริมจิตสำนึกการเขียนโปรแกรมที่ปลอดภัยสำ หรับนักพัฒนา กำหนดให้นักพัฒนาปฏิบัติตามมาตรฐานการเข้า รหัสที่ปลอดภัยอย่างเคร่งครัด • การวิเคราะห์ความต้องการ: สื่อสารเกี่ยวกับเนื้อหาและกระบวนการธุรกิจ และกรอบทางเทคนิค เพื่อค้นหาวิธีที่ดีที่สุดในการฝังความปลอดภัย • การออกแบบระบบ: สร้างแบบจำลองภัยคุกคามสำหรับการออกแบบร บบ และประเมินความปลอดภัยทางเทคนิคของสถาป ปัตยกรรมที่ใช้ • การพัฒนาระบบ: ในระหว่างกระบวนการพัฒนา จัดเตรียมส่วนประกอบการพัฒนาความปลอดภัย ที่ Tencent ออกแบบเองสำหรับนักพัฒนาใช้ และเขียนโค้ดตามมาตรฐานการเข้ารหัสความปล อดภัยของ Tencent Cloud • การยืนยันความปลอดภัย: ค้นพบช่องโหว่ผ่านการตรวจสอบความปลอดภัย ของโค้ด การสแกนความปลอดภัยของสินทรัพย์ การสแกนเว็บ การประเมินความปลอดภัยด้วยมนุษย์ การทดสอบเจาะระบบ และการตรวจสอบโค้ด • การเผยแพร่: ระบบจะเผยแพร่ไปยังสภาพแวดล้อมออนไลน์ได้ก็ ต่อเมื่อความเสี่ยงสูงทั้งหมดได้รับการแก้ไขแล้ว

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		เทคนิค (technical specification) รวมถึงต้องควบคุมการรักษา ความมั่นคงปลอดภัยและความลับของ ข้อมูลสำคัญที่นำไปใช้ในการทดสอบ	เพื่อป้องกันไม่ให้เกิดผลกระทบทำงานในสภาพแวดล้อมการผลิตโดยมีช่องโหว่ด้านความปลอดภัย
	(จ) มีการทดสอบประสิทธิภาพ (performance test) สำหรับระบบที่เกี่ยวข้องกับการ ให้บริการหรือการทำธุรกรรมทางอิเล็กทรอนิกส์		นอกจากนี้ Tencent Cloud รับรองว่าสภาพแวดล้อมการพัฒนา/ทดสอบและสภาพ แวดล้อมการผลิตถูกแยกออกจากกัน และห้ามใช้ข้อมูลการผลิตที่ยังไม่ได้ปิดในสภาพแวดล้อมการพัฒนา/ทดสอบ Tencent Cloud ยังได้กำหนดกลไกนโยบายการให้สิทธิ์และการแยกเมทริกซ์สิทธิ์ในการควบคุมการเข้าถึงภายใน
	(ข) การจัดทำคู่มือและอบรมผู้ใช้งานระบบและผู้ดูแลระบบ		เพื่อรับรองการแยกหน้าที่ระหว่างบุคลากรที่เกี่ยวข้องกับการพัฒนาซอฟต์แวร์ การทดสอบ และการเผยแพร่
			สำหรับการใช้ผลิตภัณฑ์บุคคลที่สาม Tencent Cloud ได้กำหนดข้อกำหนดด้านการจัดการความปลอดภัยของซัพพลายเชน โดยกำหนดให้ต้องมีการตรวจสอบการอนุญาตเข้าความปลอดภัยเมื่อนำเข้าองค์ประกอบภายนอก และจำเป็นต้องมีการเสริมความแข็งแกร่งด้านความปลอดภัยและการป้องกันก่อนการเปิดใช้งาน เพื่อให้มั่นใจว่าผลิตภัณฑ์ผ่านการตรวจสอบความปลอดภัยก่อนเปิดใช้งาน หลังผลิตภัณฑ์เปิดใช้งาน จะดำเนินการปฏิบัติการและบำรุงรักษาความปลอดภัยและการตรวจสอบความปลอดภัยอย่างต่อเนื่อง เพื่อแก้ไขปัญหาด้านความปลอดภัยได้ทันที่ และผ่านการประเมินสถานการณ์การดำเนินงานด้านความปลอดภัยของผลิตภัณฑ์ เพื่อระบุความเสี่ยงด้านความปลอดภัยและกระตุ้นให้ซัพพลายเออร์ปรับปรุง ตลอดจนทบทวนกลยุทธ์ความร่วมมือกับซัพพลายเออร์ดังกล่าวในอนาคต นอกจากนี้ Tencent Cloud ยังได้สร้างมาตรฐานการจัดการความปลอดภัยของส่วนประกอบโอเพนซอร์ส เพื่อให้มั่นใจว่าแหล่งที่มาของส่วนประกอบโอเพนซอร์สที่ทีมพัฒนานำเข้ามามีความน่าเชื่อถือ และผ่านการตรวจสอบความปลอดภัย เพื่อให้มั่นใจในความปลอดภัยและความถูกต้องตามกฎหมายในการใช้ส่วนประกอบโอเพนซอร์ส

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
23	การจัดการบุคคลที่สาม	ในกรณีที่บริษัทมีการจัดจ้างผู้ให้บริการภายนอก (third party management) หรือมีพันธมิตรทางธุรกิจที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของบริษัท หรือสามารถเข้าถึงข้อมูลสำคัญของบริษัท หรือของลูกค้าของบริษัทได้ บริษัทต้องมีการกำหนดกระบวนการและหลักเกณฑ์ ในการประเมินและคัดเลือกผู้ให้บริการภายนอก โดยต้องจัดทำสัญญาจ้างในการให้บริการ และกำหนดเงื่อนไขให้ผู้ให้บริการภายนอกปฏิบัติตามนโยบายการรักษาความปลอดภัยของบริษัท รวมถึงต้องกำหนดข้อตกลงระดับการให้บริการ (service level agreement : SLA) พร้อมทั้งมีการตรวจสอบและติดตามการให้บริการอย่างสม่ำเสมอ ทั้งนี้ การใช้บริการเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT outsourcing) บริษัทสามารถพิจารณาแนวทางในการดำเนินการตามแนวปฏิบัติของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยว่าด้วยหลักเกณฑ์การกำกับดูแลการใช้บริการจากผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ	หากลูกค้าจ้างผู้ให้บริการบุคคลที่สามหรือร่วมมือกับพันธมิตรทางธุรกิจ ควรกำหนดมาตรฐานการประเมินและคัดเลือกผู้ให้บริการบุคคลที่สามดังกล่าวให้ชัดเจน ทำข้อตกลงการบริการกับพวกเขา และตรวจสอบและเฝ้าระวังบริการของพวกเขาอย่างสม่ำเสมอ Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสองฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการ และสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้ บริการคลาวด์ที่ Tencent Cloud มอบให้แก่ลูกค้ามีการส่งมอบตามข้อตกลงระดับการให้บริการ (SLA) ที่ตกลงกันสำหรับแต่ละบริการ ตัวชี้วัดประสิทธิภาพ เกณฑ์การวัด และข้อกำหนดในการรายงานสำหรับบริการแต่ละรายการกำหนดไว้อย่างชัดเจนใน SLA ของผลิตภัณฑ์แต่ละรายการ และเผยแพร่บนเว็บไซต์อย่างเป็นทางการของ Tencent Cloud Tencent Cloud จะติดตามประสิทธิภาพและความพร้อมใช้งานของบริการคลาวด์อย่างต่อเนื่อง และให้การตรวจสอบแบบเรียลไทม์แก่ลูกค้าผ่านคอนโซลการจัดการ สำหรับเนื้อหารายละเอียดเพิ่มเติมเกี่ยวกับการจัดการความเสี่ยงของบุคคลที่สาม โปรดดูที่ "5.7 แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก" ในคู่มือนี้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
24	การจัดการเหตุการณ์และปัญหาด้านเทคโนโลยีสารสนเทศ	บริษัทต้องจัดให้มีการบริหารจัดการเหตุการณ์ผิดปกติและปัญหา (IT incident and problem management) ที่เกิดจากการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสมและทันที่ โดยจัดให้มีวิธีปฏิบัติ ขั้นตอนปฏิบัติ หรือแผนรองรับ ในการบริหารจัดการเหตุการณ์ผิดปกติและปัญหา ๑๓ ที่เกิดจากการใช้เทคโนโลยีสารสนเทศ รวมถึงต้องมีการบันทึก วิเคราะห์ และรายงานเหตุการณ์ผิดปกติ M น และปัญหา และการแก้ไขให้คณะกรรมการบริษัท หรือคณะกรรมการชด้อยที่ ได้รับมอบหมายทราบ ในระยะเวลาที่เหมาะสม ทั้งนี้ บริษัทต้องมีการวิเคราะห์สาเหตุที่แท้จริง (root cause) ของปัญหา เพื่อหาแนวทางแก้ไขจากสาเหตุที่แท้จริง และป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำในอนาคต	ลูกค้าควรสร้างขั้นตอนการจัดการเหตุการณ์ความปลอดภัยเทคโนโลยีสารสนเทศ เพื่อบันทึก วิเคราะห์ และรายงานเหตุการณ์ความปลอดภัย และดำเนินการวิเคราะห์สาเหตุรากฐานของเหตุการณ์ความปลอดภัยเป็นประจำ เพื่อป้องกันไม่ให้เกิดปัญหาดังกล่าวเกิดขึ้นอีก เพื่อสนับสนุนลูกค้าในการตรวจจับและตอบสนองต่ออุบัติเหตุอย่างรวดเร็ว Tencent Cloud ให้บริการแพลตฟอร์มการจัดการความปลอดภัยแบบครบวงจร Cloud Security Center (CSC) ผ่านฟังก์ชันต่างๆ เช่น ศูนย์สินทรัพย์ ศูนย์ความเสี่ยง ศูนย์แจ้งเตือน และการจัดการความปลอดภัยขั้นสูง ช่วยลูกค้าบรรลุวงจรการดำเนินงานความปลอดภัย ได้แก่ การตรวจจับภัยคุกคามก่อนเกิดเหตุการณ์ การตอบสนองและจัดการระหว่างเกิดเหตุ และการวิเคราะห์ย้อนหลังหลังเหตุการณ์ เพื่อเพิ่มประสิทธิภาพการดำเนินงานด้านความปลอดภัย ในด้านการตรวจจับและตอบสนองต่อเหตุการณ์ Tencent Cloud ได้สร้างขั้นตอนการจัดการเหตุการณ์โดยละเอียด โดยใช้ระบบการดำเนินงานความปลอดภัยภายในเพื่อบันทึกเหตุการณ์ความปลอดภัย สำหรับเหตุการณ์ความปลอดภัยที่ตรวจจับและระบุได้ Tencent Cloud จะวิเคราะห์และจำแนกระดับเหตุการณ์โดยพิจารณาจากปัจจัยต่างๆ เช่น ลักษณะของเหตุการณ์ ระดับความอ่อนไหวของข้อมูล และขอบเขตของผลกระทบ และจะแจ้งให้ผู้รับผิดชอบที่เกี่ยวข้องทราบทันทีเพื่อดำเนินการจัดการเหตุการณ์ ที่มีความปลอดภัยของ Tencent Cloud ใช้ระบบการดำเนินงานความปลอดภัยแบบ 24 ชั่วโมงทุกวัน โดยมุ่งเน้นไปที่สถานการณ์หลัก เช่น การเฝ้าระวังช่องโหว่ การติดตามแหล่งที่มาของการบุกรุก และการปิดกั้นการโจมตี ตอบสนองต่อการแจ้งเตือนความปลอดภัยแบบเรียลไทม์ และจัดทำแผนการติดตามแหล่งที่มาของการโจมตีและการจัดการเหตุการณ์ฉุกเฉินอย่างรวดเร็ว เพื่อยับยั้งการแพร่กระจายของเหตุการณ์ความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ได้อย่างมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้เหลือน้อยที่สุด ในด้านการสรุปเหตุการณ์และการปรับปรุงอย่างต่อเนื่อง Tencent Cloud ได้สร้างกลไกการวิเคราะห์เหตุการณ์เป็นระยะ โดยจะวิเคราะห์เหตุการณ์หลายมิติเป็นประจำ (ประเภทเหตุการณ์ ความถี่ในการเกิด ขอบเขตผลกระทบ และระดับความรุนแรง) และดำเนินมาตรการป้องกันตามการทบทวนเหตุการณ์และการวิเคราะห์สาเหตุรากฐาน เพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่คล้ายคลึงกันเกิดขึ้นอีก สำหรับเหตุการณ์ความปลอดภัยที่สำคัญ Tencent Cloud จะจัดตั้งทีมเฉพาะกิจเพื่อจัดทำรายงานการวิเคราะห์เฉพาะเรื่องเสนอต่อฝ่ายบริหาร สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการเหตุการณ์ด้านความปลอดภัยข้อมูล โปรดดูเนื้อหาในข้อ "11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ในคู่มือนี้
25	ความต่อเนื่องทางธุรกิจ	บริษัทต้องจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT continuity planning) โดยจะต้องมีการดำเนินการอย่างน้อยดังต่อไปนี้ (๑) จัดให้มีกระบวนการสำรองข้อมูลที่ครอบคลุมระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบงานระบบปฏิบัติการ และฐานข้อมูล เป็นต้น	ลูกค้าควรจัดทำกลไกการจัดการความต่อเนื่องของเทคโนโลยีสารสนเทศ สร้างขั้นตอนการสำรองข้อมูลและทดสอบข้อมูลสำรองเป็นประจำเพื่อให้แน่ใจว่าข้อมูลสำรองพร้อมใช้งาน ลูกค้ายังควรจัดทำและบำรุงรักษาแผนการกู้คืนจากภัยพิบัติสำหรับระบบสารสนเทศ และฝึกซ้อมทดสอบแผนดังกล่าวเป็นประจำ ในด้านการสำรองข้อมูล ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud ให้มา เช่น บริการคอมพิวเตอร์ บริการเครือข่าย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		โดยต้องรองรับการกู้คืนข้อมูลตามคว าม เหมาะสมทางธุรกิจ (๒) จัดเก็บข้อมูลสำรองไว้ในสถานที่ อย่างปลอดภัย โดยบริษัทต้องมีการเฝ้าติดตาม กระบวนการสำรองข้อมูลที่สำคัญ รวมถึงทดสอบการกู้คืนข้อมูลสำรอง และดำเนินการให้ข้อมูลสำรอง พร้อมใช้งานอยู่เสมอ (๓) จัดทำแผนการกู้คืนระบบสารสนเทศ (disaster recovery plan) เป็นลายลักษณ์อักษร โดยจะต้องมีการอนุมัติ และสื่อสารให้บุคลากรของบริษัทรับทราบ รวมถึงต้องมีการทบทวนอย่างสม่ำเสมอ หรือเมื่อมีการปรับปรุงแก้ไขที่เป็นสาระ สำคัญ (๔) จัดให้มีการทดสอบแผนการกู้คืนระบบ สารสนเทศอย่างน้อยปีละหนึ่งครั้ง และรายงานผล การทดสอบต่อผู้บริหารของบริษัทให้รับ ทราบ	บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ ไม่เพียงแต่สามารถจัดเตรียมสถาปัตยกรรมระบบที่มีคว ามพร้อมใช้งานสูงให้แก่ลูกค้า แต่ยังสนับสนุนให้ลูกค้ากำหนดกลยุทธ์การสำรองข้อมูล สำหรับระบบและข้อมูลของตนเอง ตอบสนองความต้องการสำรองข้อมูลทุกประเภทของลูก ค้า สำหรับข้อมูลของลูกค้าที่จัดเก็บไว้บนคลาวด์ Tencent Cloud ใช้วิธีการสำรองข้อมูลแบบเรียลไทม์ การเก็บข้อมูลสำรองหลายชุด และการสำรองข้อมูลข้ามพื้นที่ เพื่อรับประกันความปลอดภัยและความน่าเชื่อถือของข้อมูล ธุรกิจที่ลูกค้าเก็บไว้บนคลาวด์ รวมถึงความพร้อมใช้งานอย่างต่อเนื่อง Tencent Cloud ยังใช้มาตรการป้องกันหลายประการ เช่น ความปลอดภัยทางกายภาพ การควบคุมการเข้าถึง การแยกทางตรรกะ และสนับสนุนให้ลูกค้าใช้ Key Management Service (KMS) และ Cloud Access Management (CAM) เพื่อป้องกันไม่ให้อุปกรณ์สำรองของลูกค้าถูกเข้าถึงหรือแก้ไขโดยไม่ได้รับอนุญาต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการสำรองข้อมูล โปรดดูเนื้อหาในข้อ "8.6 การสำรองข้อมูล" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ๓ ในคู่มือนี้ เพื่อให้มั่นใจว่าลูกค้าสามารถตอบสนองและกู้คืน ฟังก์ชันสำคัญได้อย่างรวดเร็วหลังเกิดเหตุการณ์ภัยพิบัติ ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud ให้มา เช่น บริการคอมพิวเตอร์ บริการเครือข่าย บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ บริการความปลอดภัย ล้วนมีคุณลักษณะความพร้อมใช้งานสูง และมีแผนการกู้คืนจากภัยพิบัติที่สอดคล้องกัน เช่น: • Cloud Load Balancer (CLB) ให้บริการกระจายปริมาณข้อมูลระดับ 4 และ 7 ที่ปลอดภัยและรวดเร็ว โดยขยายความสามารถในการให้บริการภายนอก ของระบบแอปพลิเคชันผ่านการกระจายปริมาณ ข้อมูล และขจัดจุดล้มเหลวเพียงจุดเดียว CLB

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ใช้การปรับใช้แบบคลัสเตอร์ และจะลบอินสแตนซ์ที่ขัดข้องออกทันที เพื่อให้บรรลุความพร้อมใช้งานสูง <u>Cloud Virtual Machine (CVM)</u> มีคุณลักษณะของความพร้อมใช้งานสูงของบริการและความน่าเชื่อถือสูงของข้อมูล Cloud Block Storage ที่ใช้กับ CVM ให้กลยุทธ์การจัดเก็บข้อมูลสำรองสามชุด ซึ่งรับประกันความสามารถในการย้ายและกู้คืนข้อมูลได้อย่างรวดเร็วเมื่อสำเนาใดสำเนาหนึ่งขัดข้อง <u>Cloud Object Storage (COS)</u> ให้การจัดเก็บข้อมูลสำรองหลายชุดผ่านหลายสถาปัตยกรรมและหลายอุปกรณ์ จัดเตรียมฟังก์ชันการกู้คืนจากภัยพิบัติข้ามพื้นที่และการแยกทรัพยากรสำหรับข้อมูลลูกค้า และให้บรรลุความคงทนของข้อมูล <u>TencentDB for MySQL</u> รองรับความน่าเชื่อถือสูงของข้อมูลและความพร้อมใช้งานสูงของบริการ และมีกลไกการสำรองข้อมูลอัตโนมัติและการกู้คืนโดยไม่สูญเสียข้อมูลที่สมบูรณ์ <u>Tencent Kubernetes Engine (TKE)</u> ใช้สถาปัตยกรรมบริการแบบกระจาย รับประกันการกู้คืนโดยอัตโนมัติจากการขัดข้องของบริการและการย้ายถิ่นฐานอย่างรวดเร็ว ผสานกับที่เก็บข้อมูลแบบกระจายสำหรับบริการแบบมีสถานะ (Stateful) เพื่อให้บรรลุความปลอดภัยและความพร้อมใช้งานสูงของบริการและข้อมูล เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud มีการแยกจากกันโดยสมบูรณ์ระหว่างภูมิภาคต่างๆ เพื่อรับประกันความเสถียรและความทนทานต่อข้อผิดพลาดสูงสุดระหว่างภูมิภาคต่างๆ เพื่อให้มั่นใจในความพร้อมใช้งานสูงของข้อมูล Tencent Cloud แบ่งแต่ละภูมิภาคออกเป็นหลาย Availability Zone ที่แยกจากกัน การออกแบบหลาย Availability Zone ของ Tencent Cloud สามารถลดผลกระทบจากความล้มเหลวของจุดเดียวได้อย่างมีประสิทธิภาพ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และรับประกันว่าความล้มเหลวระหว่าง Availability Zone จะถูกแยกจากกัน ซึ่งจะช่วยรับประกันความต่อเนื่องของธุรกิจของลูกค้า เพื่อให้มั่นใจในความพร้อมใช้งานอย่างต่อเนื่องของธุรกิจลูกค้า Tencent Cloud ได้ออกแบบและนำกรอบการจัดการความต่อเนื่องของธุรกิจที่เหมาะสมกับสภาพแวดล้อมคอมพิวเตอร์คลาวด์ของตนเองไปใช้ และได้รับใบรับรองมาตรฐานสากล ISO/IEC 22301 สำหรับระบบการจัดการความต่อเนื่องของธุรกิจ Tencent Cloud จะดำเนินการวิเคราะห์ผลกระทบทางธุรกิจสำหรับผลิตภัณฑ์และบริการคลาวด์ กำหนด RTO และ RPO ของแต่ละธุรกิจให้ชัดเจน และจัดทำกลยุทธ์การตอบสนองและแผนความต่อเนื่องของธุรกิจที่แตกต่างกันตามผลการวิเคราะห์ผลกระทบทางธุรกิจ รวมถึงจัดทำแผนฉุกเฉินสำหรับการกู้คืนจากภัยพิบัติโดยละเอียดสำหรับผลิตภัณฑ์คลาวด์ Tencent Cloud จะทำการทดสอบฝึกซ้อมความต่อเนื่องของธุรกิจสำหรับผลิตภัณฑ์คลาวด์เป็นประจำตามแผนความต่อเนื่องของธุรกิจ เพื่อให้มั่นใจในความสามารถในการปฏิบัติได้จริงของแผน แผนฉุกเฉิน ฯลฯ

14.2 การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
27	แนวทางการจัดการความเสี่ยงด้านเทคโนโลยี	บริษัทต้องจัดให้มีแนวทางในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่ระบุขอบเขตและเกณฑ์การบริหารความเสี่ยงอย่างน้อย ดังต่อไปนี้ (๑)การพิจารณาโอกาสและความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยการระบุขอบเขตและขอบเขตในการประเมินความเสี่ยงให้ครอบคลุมถึง แผนงาน งานประจำ และการนำเทคโนโลยี สารสนเทศมาใช้	ลูกค้าควรกำหนดกรอบการจัดการความเสี่ยง ซึ่งควรรวมถึงบริบทและขอบเขตของการประเมินความเสี่ยง การกำหนดมาตรฐานการจัดการความเสี่ยง การกำหนดระดับความชอบในความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Appetite) การกำหนดขั้นตอนการประเมินความเสี่ยง และกลไกการจัดการความเสี่ยง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามงานต่างๆ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		๑๔ (๒)เกณฑ์การบริหารความเสี่ยงที่มีราย ละเอียดเกี่ยวกับเกณฑ์การประเมินค ความเสี่ยง โดยกำหนดระดับของผลกระทบและระ ดับของโอกาสการเกิดเหตุการณ์ (๓)ระดับความเสี่ยงที่ยอมรับได้สำหรับ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk apptt) (๔) กระบวนการประเมินความเสี่ยง เพื่อใช้ในการระบุ วิเคราะห์ และประเมินผลความเสี่ยง (๕) กระบวนการจัดการความเสี่ยง เพื่อใช้พิจารณาทางเลือก และมาตรการในการจัดการ ความเสี่ยง รวมถึงการจัดทำแผนบริหารจัดการคว ามเสี่ยง	เช่น การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยงไว้อย่างชัดเจน Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุความเสี่ยงตามสถานการณ์ความเสี่ยง ผลิตภัณฑ์ทางธุรกิจ หรือกระบวนการให้บริการ สำหรับความเสี่ยงที่ระบุได้ Tencent Cloud จะประเมินความเป็นไปได้และระดับผลกระทบของความ เสี่ยงแต่ละรายการเพื่อจำแนกระดับความเสี่ยง และดำเนินการตามขั้นตอนที่สอดคล้องกันต่อไป โดยมีการบันทึกกิจกรรมกระบวนการทั้งหมดไว้ Tencent Cloud ยังติดตามสถานการณ์การจัดการความเสี่ยงอย่างต่อเนื่อง ประเมินความเสี่ยงที่เหลืออยู่ และให้มั่นใจว่าผู้เกี่ยวข้องได้จัดการความเสี่ยงอย่างเหม อะสมตามข้อกำหนดการจัดการความเสี่ยงของ Tencent Cloud นอกจากนี้ Tencent Cloud บำรุงรักษาและปรับปรุงวิธีการประเมินความเสี่ยงและทะ เบียนความเสี่ยงอย่างต่อเนื่องตามแนวโน้มการเปลี่ยนแ ปลงในอุตสาหกรรมคลาวด์และแนวปฏิบัติการจัดการภ ายใน
28	การประเมินค ความเสี่ยงด้าน เทคโนโลยีสาร สนเทศ	บริษัทต้องจัดให้มีการประเมิน ความเสี่ยง (risk assessment) ด้านเทคโนโลยี สารสนเทศ ตามหลักเกณฑ์และวิธีการ ดังต่อไปนี้ (๑) ระบุความเสี่ยง (risk identification) ด้านเทคโนโลยีสารสนเทศ ซึ่งรวมถึงภัยคุกคาม ทางไซเบอร์ และช่องโหว่ที่สำคัญ โดยเหตุการณ์ความเสี่ยงดังกล่าวอาจ มีสาเหตุมาจากกระบวนการ ปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก ตลอดจนระบุการควบคุมที่มีอยู่ในปัจจุ บัน และ ผู้รับผิดชอบหรือเจ้าของความเสี่ยง (risk owners) (๒) วิเคราะห์ความเสี่ยง (risk analysis) ด้านเทคโนโลยีสารสนเทศ	ลูกค้าควรระบุภัยคุกคามและช่องโหว่ที่ใช้ได้กับสภาพ แวดล้อมเทคโนโลยีสารสนเทศของตนเป็นประจำ วิเคราะห์และประเมินความเสี่ยงที่เกิดจากภัยคุกคามแล ะช่องโหว่เหล่านี้ จัดลำดับความสำคัญของความเสี่ยง จัดทำมาตรการลดความเสี่ยง ประเมินความเสี่ยงที่เหลืออยู่ และติดตามประสิทธิภาพของมาตรการควบคุมความเสี่ยง Tencent Cloud ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัย ดภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามและให้คำแนะนำเกี่ยวกับเนื้อหาการทำ งานของกระบวนการจัดการความเสี่ยงทั้งหมด (การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยง) ไว้อย่างชัดเจน • การระบุความเสี่ยง: Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุสถานการณ์ความเสี่ยงที่ใช้ได้กับ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
29	การจัดการ/ต อบสนองต่อค วามเสี่ยง	โดยมีการประเมิน ระดับของผลกระทบ และระดับของโอกาสการเกิดเหตุการณ์ เพื่อจัดลำดับความสำคัญของความเสี่ยง (๓) ประเมินค่าความเสี่ยง (risk evaluation) โดยการพิจารณาระดับความเสี่ยงกับ ระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) เพื่อจัดลำดับและหาแนวทางในการต อบสนอง ความเสี่ยงที่เหมาะสม	Tencent Cloud จากแหล่งต่างๆ เช่น รายงานเหตุการณ์ความปลอดภัยในอุตสาหกรรม การสะสมประสบการณ์การปฏิบัติของ Tencent Cloud ฐานข้อมูลความเสี่ยงของสถาบันมืออาชีพ และระบุความเสี่ยงตามผลการวิเคราะห์กระบวนการของสถานการณ์ความเสี่ยง ผลิตภัณฑ์หรือบริการทางธุรกิจ
		บริษัทต้องมีการจัดการความเสี่ยง (risk treatment) โดยมีแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ คำนึงถึง ความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยง และผลประโยชน์ที่คาดว่าจะได้รับ รวมทั้งกำหนด ดัชนีชี้วัดความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT key risk indicators) เพื่อใช้ในการติดตามและ ทบทวนความเสี่ยง	• การประเมินความเสี่ยง: Tencent Cloud ประเมินมูลค่าสินทรัพย์ ความเป็นไปได้ของความเสี่ยงในสถานการณ์ความ เสี่ยง และระดับผลกระทบของความเสี่ยง และคำนวณระดับความเสี่ยง • การจัดการความเสี่ยง: ตามผลการวิเคราะห์ความเสี่ยง สำหรับความเสี่ยงที่ระบุ Tencent Cloud จะใช้กลยุทธ์การตอบสนองและมาตรการบรรเทา ความเสี่ยงที่สอดคล้องกัน สำหรับความเสี่ยงสูง ผู้รับผิดชอบด้านความเสี่ยงจะจัดทำแผนจัดการค วามเสี่ยง (มาตรการการโอนย้ายหรือลดความเสี่ยง) และอัปเดตตารางการจัดการความเสี่ยง สำหรับความเสี่ยงปานกลาง ผู้รับผิดชอบด้านความเสี่ยงจะตัดสินใจตามสภาพแ วดล้อมจริงว่าจำเป็นต้องจัดทำแผนจัดการความ เสี่ยงหรือไม่ สำหรับความเสี่ยงต่ำถือเป็นความเสี่ยงที่ยอมรับได้ สำหรับความเสี่ยงที่เหลือ Tencent Cloud จะทบทวนทุกครั้ง เพื่อตรวจสอบสถานะและมูลค่าความเสี่ยง • การติดตาม การทบทวน และการรายงานความเสี่ยง: Tencent Cloud รวบรวมผลการประเมินความเสี่ยง ออกรายงานการประเมินความเสี่ยง และรายงานต่อฝ่ายบริหาร และบำรุงรักษาตารางการจัดการความเสี่ยง ติดตามการเปลี่ยนแปลงเงื่อนไขความเสี่ยงและส ถานะของแผนจัดการความเสี่ยง และปรับแผนการจัดการความเสี่ยงแบบเรียลไทม์
30	การตรวจสอบ และทบทวนค วามเสี่ยง	บริษัทต้องจัดให้มีกระบวนการติดตาม และทบทวนความเสี่ยง (risk monitoring and review) ด้านเทคโนโลยีสารสนเทศที่มีประสิทธิ ภาพ เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้	นอกจากนี้ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ยังกำหนดตัวชี้วัดความเสี่ยงที่สำคัญและวัดตัวชี้วัดความ เสี่ยงที่สำคัญเป็นประจำ เทียบเคียงกับเกณฑ์ความเสี่ยงที่ยอมรับได้ วิเคราะห์สาเหตุรากฐานของปัญหาที่พบ และเสนอข้อเสนอแนะและแนวทางในการปรับปรุง

14.3

การปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
32	การปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศ	บริษัทต้องจัดให้มีการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT compliance) เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และกฎหมายอื่นในลักษณะเดียวกัน เพื่อป้องกันไม่ให้เกิดการฉ้อฉลหรือไม่ปฏิบัติตามกฎหมายและหลักเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้อง	ลูกค้าควรกำกับดูแลการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ และข้อกำหนดทางการกำกับดูแลด้านเทคโนโลยีสารสนเทศของตน ในด้านการปฏิบัติตามข้อกำหนด Tencent Cloud ปฏิบัติตามกฎหมายและระเบียบข้อบังคับของเขตอำนาจศาลที่ดำเนินธุรกิจอยู่อย่างเคร่งครัด และได้สร้างขั้นตอนที่เกี่ยวข้องกับการปฏิบัติตามข้อกำหนดด้านความปลอดภัย เพื่อให้มั่นใจว่าการดำเนินการด้านความปลอดภัยข้อมูลเป็นไปตามข้อกำหนดของกฎหมาย ระเบียบข้อบังคับ มาตรฐาน และขั้นตอนที่เกี่ยวข้อง ทีมงานฝ่ายกฎหมายของ Tencent Cloud จะระบุและรวบรวมข้อกำหนดการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับธุรกิจของ Tencent Cloud อย่างต่อเนื่อง จัดทำเป็นรายการกฎหมายและระเบียบข้อบังคับที่สอดคล้องกัน และบำรุงรักษาและปรับปรุงเป็นประจำ ในด้านการตรวจสอบและการทบทวน Tencent Cloud โดยลูกค้า ในเวลาเดียวกัน ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละหนึ่งครั้ง และตรวจสอบสถานการณ์ของแพลตฟอร์มคลาวด์และระบบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามกฎหมาย ระเบียบข้อบังคับ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง Tencent Cloud ยังได้รับการตรวจสอบโดยบุคคลที่สามอิสระมืออาชีพเป็น ประจำ โดยผ่านการจัดทำรายงานการควบคุมระบบและองค์กร ที่มีลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการ ล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้องศูนย์ความปลอดภัยแพลตฟอร์มคลาวด์จะป ระเมินและยืนยันการปฏิบัติตามนโยบายและขั้นตอนคว ามปลอดภัยเป็นประจำ โดยขอบเขตการประเมินรวมถึงการรั่วไหลของข้อมูลที ละเอียดอ่อน การลดช่องโหว่ด้านความปลอดภัย การกำหนดค่าความปลอดภัย เป็นต้น

14.4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
33	หน้าที่ งาน และแผนการต รวจสอบเทคโ นยีสารสนเทศ	บริษัทต้องมีการกำหนดบทบาทหน้า ที่และแผนงานในการตรวจสอบ ด้านเทคโนโลยีสารสนเทศ โดยจะต้องมีการดำเนินการอย่างน้อ ย ดังต่อไปนี้ (๑) จัดให้มีผู้ตรวจสอบด้านเทคโนโ ยีสารสนเทศที่มีความรู้ ประสบการณ์ และความ เชี่ยวชาญเกี่ยวกับการตรวจสอบด้ านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบจากภายนอกก็ได้ (๒) ต้องจัดให้มีแผนงานและขอบเขต การตรวจสอบด้านเทคโนโลยีสารสนเทศ ที่ครอบคลุม ความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของบริษัท โดยแผนงานและขอบเขตในการตรวจ	ลูกค้าควรสร้างกลไกการตรวจสอบเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจว่าบุคลากรตรวจสอบ IT มีความสามารถและทักษะทางวิชาชีพ ดำเนินการตรวจสอบความเสี่ยงทางเทคนิคเป็นประจำ และติดตามเฝ้าระวังปัญหาที่พบในระหว่างกระบวนการตร วสอบ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับ ดูแล Tencent Cloud จะให้ความช่วยเหลือจากบุคคลเฉพาะตามสถานการณ์จ ริง ตอบสนองอย่างแข็งขัน และสนับสนุนข้อกำหนดในการตรวจสอบและกำกับดูแล Tencent Cloud จากลูกค้าและหน่วยงานกำกับดูแลทางการเงินของประเท ศไทย ทีมงานด้านความปลอดภัยของ Tencent Cloud จะเฝ้าติดตามและประเมินความเสี่ยงด้านความปลอดภัยก ายในอย่างต่อเนื่อง เพื่อรับประกันประสิทธิภาพและความน่าเชื่อถือของระบบกา

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
34	งานตรวจสอบ เทคโนโลยีสาร สนเทศ	ตรวจสอบต้องได้รับ ความเห็นชอบจากคณะกรรมการ ตรวจสอบ และต้องจัดให้มีการทบทวนอย่างน้อย ปีละหนึ่งครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัย สำคัญ	จัดการความปลอดภัยข้อมูล ทีมงานด้านความปลอดภัยของ Tencent Cloud ดำเนินการตรวจสอบความปลอดภัยภายในอย่างน้อยปีละ หนึ่งครั้ง และเฝ้าติดตามสถานการณ์ของแพลตฟอร์มคลาวด์และระ บบภายในอย่างต่อเนื่อง เพื่อให้มั่นใจว่ามีสถานะความปลอดภัยที่ดีและเป็นไปตามขอ กําหนดและกฎระเบียบ
		บริษัทต้องจัดให้มีการปฏิบัติงานตรวจ สอบด้านเทคโนโลยีสารสนเทศ โดยจะต้อง มีการดำเนินการอย่างน้อย ดังต่อไปนี้ (๑) ตรวจสอบด้านเทคโนโลยีสารสนเทศให้ เหมาะสมตามแผนงานและขอบ เขตที่กำหนด และเมื่อมีเหตุการณ์ผิดปกติด้านเทคโนโลยี สารสนเทศที่มีนัยสำคัญ (๒) ในกรณีที่ระบบเทคโนโลยีของบริษัท มีความซับซ้อนหรือเป็นเทคโนโลยีใหม่ โดยบริษัท มีข้อจำกัดที่ไม่สามารถประเมินหรือ ตรวจสอบเองได้ บริษัทสามารถจ้างผู้เชี่ยวชาญภายนอก ทำหน้าที่ ในการตรวจสอบแทนได้	รวมถึงมาตรฐานการจัดการความปลอดภัยที่เกี่ยวข้อง นอกจากนี้ Tencent Cloud ยังได้รับการตรวจสอบจากมืออาชีพโดยบุคคลที่สามที่เป็น อิสระทุกปี และโดยการจัดทำรายงานการควบคุมระบบและองค์กรที่มี ลักษณะการรับรอง จะเปิดเผยสถานะการควบคุมภายในขององค์กรให้บริการ ล่าสุดของ Tencent Cloud แก่องค์กรผู้ใช้คลาวด์ ผู้ตรวจสอบอิสระ หน่วยงานกำกับดูแล ผู้ถือหุ้นบริษัท และผู้มีส่วนได้ส่วนเสียอื่น ๆ ที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งสำหรับภูมิภาคไทย Tencent Cloud ได้ผ่านการตรวจสอบการปฏิบัติตามข้อกำหนด IT สำหรับอุตสาหกรรมการเงินไทยที่ดำเนินการโดยบุคคลที่ สามที่เป็นอิสระแล้ว ลูกค้าสามารถดาวน์โหลดรายงานล่าสุดได้ด้วยตนเองจาก " Compliance Document Download "
		บริษัทต้องจัดให้มีการรายงานผลและ ติดตามผลการตรวจสอบ โดยจะต้องมีการ ดำเนินการอย่างน้อย ดังต่อไปนี้ (๑) จัดทำรายงานผลการตรวจสอบด้ านเทคโนโลยีสารสนเทศเสนอต่อ คณะกรรมการ ตรวจสอบ และจัดเก็บรายงานผลการตรวจสอบ ดังกล่าวไว้ที่บริษัทเพื่อรองรับการตร วสอบ หรือร้องขอ จากสำนักงาน (๒) จัดให้มีการติดตามประเด็นจาก การตรวจสอบด้านเทคโนโลยีสารสนเทศ และ รายงานประเด็นสำคัญให้กับคณะกรรมการ ตรวจสอบ	จะวิเคราะห์สาเหตุจริงหรือสาเหตุที่มีศักยภาพที่ทำให้เกิด ข้อที่ไม่สอดคล้องอย่างทันท่วงที ประเมินความต้องการและลำดับความสำคัญของการดํา เนินมาตรการแก้ไขและป้องกัน และดําเนินมาตรการแก้ไขและป้องกันหลังจากได้รับอนุมัติ ที่เกี่ยวข้อง ประสิทธิภาพของการดําเนินมาตรการแก้ไขจะถูกติดตามแ ละบันทึกอย่างต่อเนื่อง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud

และฝ่ายงานที่เกี่ยวข้องทราบ

14.5

การกำกับดูแลและการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
36	แนวทางการ บริหารความม ั่นคงปลอดภัย ทางไซเบอร์	บริษัทต้องจัดให้มีแนวทางการ กำกับดูแลการเตรียมความพร้อม รับมือภัยคุกคาม ทางไซเบอร์ (cyber resilience) โดยมีกรอบการดำเนินงานและแ นทางที่ใช้ในการกำกับดูแล และ บริหารจัดการความเสี่ยงจากภ ยคุกคามทางไซเบอร์ในภาพรว มขององค์กร ที่สอดคล้องกับกฎหมาย ว่าด้วยการรักษาความมั่นคงปล อดภัยไซเบอร์ รวมทั้งเหมาะสมสอดคล้องกับข ขนาด และความซับซ้อน ของการดำเนินธุรกิจ	ลูกค้าควรจัดทำแนวทางการบริหารความมั่นคงปลอดภัยทางไ ซเบอร์ที่สอดคล้องกับขนาดและความซับซ้อนของการดำเนิน งานทางธุรกิจ สร้างกรอบการดำเนินงานและแผนปฏิบัติการที่ครอบคลุมการ จัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านกลยุทธ์ความปลอดภัยทางไซเบอร์ เพื่อรับมือกับภัยคุกคามทางเครือข่ายและความเสี่ยงด้านคว ามปลอดภัยที่ซับซ้อนมากขึ้นในยุคดิจิทัล Tencent Cloud ได้เปิดตัวกรอบแบบจำลอง "ภูมิคุ้มกันปลอดภัยดิจิทัล" เสนอให้ใช้แนวคิดด้านภูมิคุ้มกันในการรับมือกับความสัมพันธ เชิงประสานงานระหว่างการสร้างความปลอดภัยและการพัฒนา ธุรกิจในยุคใหม่ โดยกำหนดเป้าหมายที่ข้อมูลและธุรกิจขององค์กร เพื่อสร้างระบบภูมิคุ้มกันความปลอดภัยที่มีความยืดหยุ่น ปรับตัวได้ และขยายได้ ช่วยคุ้มครองการพัฒนาคุณภาพสูงขององค์กรในยุคดิจิทัล Tencent Cloud มีเป้าหมาย "เสริมสร้างภูมิคุ้มกันปลอดภัยดิจิทัลขององค์กร สนับสนุนการพัฒนาที่มีความยืดหยุ่นในยุคดิจิทัล" มุ่งมั่นปรับปรุงระบบความปลอดภัยบนคลาวด์ของตนเอง สร้างขีดความสามารถด้านความปลอดภัยและการปฏิบัติตาม ข้อกำหนด และกำหนดมาตรฐานความปลอดภัยบนคลาวด์ โดยอิงตามกรอบแบบจำลองที่วางแผนอย่างครอบคลุม ผ่านผลิตภัณฑ์ที่หลากหลายและคุณลักษณะด้านความปลอด ภัย Tencent Cloud บริหารการป้องกันในทุกด้าน และนำฟังก์ชันความปลอดภัยที่สอดคล้องกันไปใช้ในผลิตภัณฑ์ ทุกระดับ นอกจากนี้ Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะทบทวนนโยบาย/กลยุทธ์ด้านความปลอดภัยเป็นประจำ และปรับปรุงตามความต้องการตามสถานการณ์ทางธุรกิจและ การพัฒนาทางเทคโนโลยี เป็นต้น
37	การกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์	บริษัทต้องมีการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์และการระบุ ความเสี่ยง (identification) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้ (๑) กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (cybersecurity governance) (๒) จัดทำรายการทรัพย์สินสารสนเทศและบริหารจัดการทรัพย์สินสารสนเทศ (๓) กำหนดขอบเขตและวิธีการในการประเมินความเสี่ยงด้านไซเบอร์ที่สอดคล้องกับ การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือความมั่นคงปลอดภัยสารสนเทศ (๔) จัดให้มีการจัดทำแผนบริหารจัดการความเสี่ยงมาตรการจัดการ ความเสี่ยง หรือ แนวทางในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ ที่สอดคล้องกับผลการประเมิน ความเสี่ยง ด้านไซเบอร์ (๕) มีการบริหารจัดการความเสี่ยงเกี่ยวกับห่วงโซ่อุปทานให้บริกรภายนอก (supply chain risk management) แนวทางในการบริหารจัดการผู้ให้บริการภายนอก การทำสัญญาจ้าง การประเมิน	ลูกค้าควรสร้างกลไกการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ กำหนดโครงสร้างการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ให้ชัดเจน บำรุงรักษาบัญชีรายการสินทรัพย์เทคโนโลยีสารสนเทศ กำหนดกลไกการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ให้ชัดเจน และจัดทำมาตรการและแผนการจัดการความเสี่ยงตามผลการประเมิน รวมถึงจัดการความเสี่ยงในห่วงโซ่อุปทาน เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ในด้านโครงสร้างองค์กรด้านการจัดการความปลอดภัยเทคโนโลยีสารสนเทศ Tencent Cloud ได้สร้างโครงสร้างองค์กรที่เกี่ยวข้องกับความปลอดภัยบนคลาวด์และความปลอดภัยข้อมูล กำหนดบทบาทหน้าที่ด้านความปลอดภัยและความรับผิดชอบที่เกี่ยวข้องในระดับต่างๆ ให้ชัดเจน และกำหนดกลไกการทำงานสำหรับการตรวจสอบความปลอดภัยข้อมูลและการประเมินความเสี่ยงด้านความปลอดภัยข้อมูล Tencent Cloud ได้จัดตั้งคณะกรรมการเทคโนโลยีความปลอดภัยและทีมงานความปลอดภัยมีอาชีพที่มีหน้าที่และสาขาวิชาที่แตกต่างกัน Tencent Cloud รวบรวมทีมบริการผู้เชี่ยวชาญที่มีประสบการณ์ในอุตสาหกรรม มุ่งมั่นให้บริการผลิตภัณฑ์และบริการที่ปลอดภัย นำเชื่อถือ เป็นมืออาชีพ และเป็นไปตามข้อกำหนดแก่ลูกค้า Tencent Cloud ยังกำหนดองค์ประกอบของเจ้าหน้าที่ประสานงานด้านความปลอดภัยข้อมูล (Information Security Liaison Officer) โดยเจ้าหน้าที่ประสานงานด้านความปลอดภัยข้อมูลในแต่ละภูมิภาคจะรักษาการสื่อสารที่ราบรื่นกับหน่วยงานกำกับดูแลท้องถิ่นและลูกค้าตามข้อกำหนดการปฏิบัติตามและความต้องการทางธุรกิจ เพื่อให้มั่นใจว่า Tencent Cloud ปฏิบัติตามกฎหมาย กฎระเบียบ และข้อตกลงตามสัญญา ในการจัดการสินทรัพย์ Tencent Cloud ได้กำหนดมาตรฐานการจัดการสินทรัพย์ข้อมูลและกระบวนการ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ความเหมาะสม การติดตามและประเมินผลการ ปฏิบัติงาน และการสอบทานผลการปฏิบัติงาน	การจัดการตลอดวงจรชีวิตสินทรัพย์ เพื่อจัดการและปกป้องสินทรัพย์ เช่น ข้อมูลอิเล็กทรอนิกส์ ฮาร์ดแวร์และอุปกรณ์เสมือน โครงสร้างพื้นฐาน ระบบแอปพลิเคชัน และซอฟต์แวร์ โดยจำแนกประเภทและระดับ Tencent Cloud ใช้ระบบการจัดการสินทรัพย์ในการบริหารจัดการอุปกรณ์ฮาร์ดแวร์และส่วนประกอบซอฟต์แวร์ รวมถึงการลงทะเบียนและผูกมัดสินทรัพย์ การตรวจนับและการอัปเดตข้อมูลสินทรัพย์ การปลดระวางและเปลี่ยนใหม่สินทรัพย์ เป็นต้น เพื่อรับประกันการทำงานที่ราบรื่นของระบบพื้นฐานของแพลตฟอร์มคลาวด์ และจัดเตรียมการสนับสนุนที่เชื่อถือได้ให้กับระบบธุรกิจ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการสินทรัพย์ โปรดดูเนื้อหาในข้อ "16 การจัดการสินทรัพย์เทคโนโลยีสารสนเทศ" ของ "14.1 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้ สำหรับด้านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามงานต่างๆ เช่น การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยงไว้อย่างชัดเจน Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุความเสี่ยงตามสถานการณ์ความเสี่ยง ผลิตภัณฑ์ทางธุรกิจ หรือกระบวนการให้บริการ สำหรับความเสี่ยงที่ระบุได้ Tencent Cloud จะประเมินความเป็นไปได้และระดับผลกระทบของความเสี่ยงแต่ละรายการเพื่อจำแนกระดับความเสี่ยง และดำเนินการตามขั้นตอนที่สอดคล้องกันต่อไป โดยมีการบันทึกกิจกรรมกระบวนการทั้งหมดไว้ Tencent Cloud ยังติดตามสถานการณ์การจัดการความเสี่ยงอย่างต่อเนื่อง ประเมินความเสี่ยงที่เหลืออยู่ และให้มั่นใจว่าผู้เกี่ยวข้องได้จัดการความเสี่ยงอย่างเหมาะสมตามข้อกำหนดการจัดการความเสี่ยงของ Tencent Cloud นอกจากนี้ Tencent Cloud บำรุงรักษาและปรับปรุงวิธีการประเมินความเสี่ยงและทะเบียนค

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ความเสี่ยงอย่างต่อเนื่องตามแนวโน้มการเปลี่ยนแปลงในอุตสาหกรรมคลาวด์และแนวปฏิบัติการจัดการภายใน ในด้านการจัดการห่วงโซ่อุปทาน Tencent Cloud จะให้ความร่วมมือตามสถานการณ์จริงและตามข้อตกลงที่ตกลงกับลูกค้า ในการตรวจสอบความปลอดภัยและการกำกับดูแลของบุคคลที่สามของลูกค้า และจัดเตรียมผู้เชี่ยวชาญเฉพาะทางเพื่อตอบสนองและสนับสนุนกิจกรรมการตรวจสอบที่ลูกค้าเป็นผู้ริเริ่มอย่างเข้มข้น Tencent Cloud จัดเตรียมเอกสารกฎหมายออนไลน์บนเว็บไซต์อย่างเป็นทางการระหว่างประเทศ เช่น Terms of Service Service Level Agreement (SLA) Data Processing and Security Agreement ซึ่งกำหนดรายละเอียดเนื้อหาและระดับการให้บริการที่ Tencent Cloud มอบให้ การปกป้องข้อมูลผู้ใช้และทรัพย์สินทางปัญญา ความรับผิดชอบและหน้าที่ด้านความปลอดภัยของทั้งสองฝ่ายระหว่างลูกค้าและ Tencent Cloud ระยะเวลาการให้บริการและสถานการณ์การสิ้นสุดข้อตกลง อย่างชัดเจน ลูกค้ายังสามารถเลือกทำสัญญากับ Tencent Cloud แบบออฟไลน์ เพื่อเจรจาข้อกำหนดและรายละเอียดในสัญญาได้
38	การป้องกันความเสี่ยง	บริษัทต้องมีการป้องกันความเสี่ยง (protection) โดยต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้ (๑) กำหนดแนวทางการควบคุมและป้องกันความเสี่ยงของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของบริษัท เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และ ระบบงาน เป็นต้น รวมทั้งการตั้งค่าระบบงาน การเข้าถึงระบบงานและการจัดการสิทธิ์ การรักษาความมั่นคงปลอดภัยของข้อมูล การพัฒนาระบบงานที่มีความปลอดภัย	ลูกค้าควรกำหนดมาตรการป้องกันความเสี่ยง จัดทำกลไกการจัดการการกำหนดค่าระบบ การจัดการการเข้าถึงแอปพลิเคชัน การจัดการความปลอดภัยของข้อมูล การจัดการความปลอดภัยในการพัฒนาระบบ และการจัดการแพตช์สำหรับโครงสร้างพื้นฐานสารสนเทศที่สำคัญ รักษาขั้นตอนการปฏิบัติงานด้านความปลอดภัยเครือข่าย และเสริมสร้างการรวบรวมและการวิเคราะห์ข้อมูลภัยคุกคามความปลอดภัยเครือข่าย สำหรับการจัดการการกำหนดค่าระบบโครงสร้างพื้นฐานสารสนเทศที่สำคัญ Tencent Cloud ได้กำหนดมาตรฐานการกำหนดค่าความปลอดภัยเครือข่ายและมาตรฐานเส้นฐานความปลอดภัยขึ้น เพื่อจัดการมาตรฐานการกำหนดค่าความปลอดภัยของอุปกรณ์เครือข่าย ไฟร์วอลล์ ระบบปฏิบัติการของเซิร์ฟเวอร์โฮสต์ ฐานข้อมูล และระบบแอปพลิเคชัน Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		ลดภัยตามขั้นตอนหรือกระบวนการในการ พัฒนาระบบงาน (system development life cycle: SDLC) การบริหารจัดการ patch โดยมีการใช้เทคโนโลยีอย่างเหมาะสม เพื่อให้บริษัทมีกระบวนการเครื่องมือและวิธีการในการควบคุมหรือลดผลกระทบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น (๒)มีเอกสารการปฏิบัติงานสำหรับดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ สอดคล้องตามมาตรฐานและแนวปฏิบัติที่ดี (๓)มีแนวทางในการรวบรวมและวิเคราะห์ข้อมูลภัยคุกคามไซเบอร์ ตลอดจนกำหนดวิธีการรวมทั้งช่องทางในการแลกเปลี่ยนข้อมูลและสร้างความร่วมมือในการบริหารจัดการ และรับมือภัยคุกคามทางไซเบอร์ทั้งภายในและภายนอกองค์กร	ใช้เครื่องมือสแกนเพื่อตรวจจับความเบี่ยงเบนของการกำหนดค่าระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และอีเมลเสมือน (Virtual Image) จากมาตรฐานอย่างต่อเนื่อง สำหรับความเบี่ยงเบนที่ตรวจพบ Tencent Cloud จะสร้างใบงานความปลอดภัยและส่งไปยังทีมงานผู้รับผิดชอบโดยอัตโนมัติ เพื่อดำเนินการแก้ไขทันทีที่ Tencent Cloud ยังทบทวนนโยบายความปลอดภัยและการตั้งค่าพารามิเตอร์ของอุปกรณ์เครือข่าย เช่น เราเตอร์ ไฟร์วอลล์ และเซิร์ฟเวอร์เครือข่าย เป็นระยะ เพื่อให้มั่นใจในประสิทธิภาพของนโยบายและพารามิเตอร์สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการกำหนดค่าโปรดดูเนื้อหาในข้อ "8.1 การบริหารจัดการการตั้งค่าระบบ" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้ ในด้านการจัดการการเข้าถึง Tencent Cloud ยังได้กำหนดกลยุทธ์การให้สิทธิ์การควบคุมการเข้าถึงและกลไกการแบ่งแยกสิทธิ์ภายในองค์กร Tencent Cloud ใช้ระบบจัดการความปลอดภัยแบบ Zero-Trust ในการตรวจสอบสิทธิ์การเข้าถึงของพนักงาน โดยผู้ใช้ต้องผ่านการยืนยันตัวตนสองปัจจัยก่อนเข้าถึงทรัพยากรภายใน Tencent Cloud ปฏิบัติตามหลักการสิทธิ์น้อยที่สุดอย่างเคร่งครัด และใช้การควบคุมสิทธิ์น้อยที่สุดโดยค่าเริ่มต้น พนักงานจะได้รับสิทธิ์เฉพาะที่ต่อเมื่อมีความจำเป็นต้องใช้ และผ่านกระบวนการอนุมัติสิทธิ์ที่เข้มงวดเท่านั้น Tencent Cloud จะรักษานโยบายข้อมูลตัวตนของบุคลากรที่สอดคล้องกับบทบาทหน้าที่และระดับสิทธิ์ในระบบธุรกิจต่างๆ และด้วยการจัดงานตรวจสอบสิทธิ์ภายในเป็นประจำ เพื่อให้มั่นใจว่าสิทธิ์จะไม่ถูกใช้ในทางที่ผิดหรือใช้ผิดวัตถุประสงค์ สภาพแวดล้อมการผลิตของ Tencent Cloud ได้ปรับใช้เครื่องบินคุ้มกัน อย่างเต็มรูปแบบ โดยควบคุมสิทธิ์บัญชีผู้ดูแลระบบของส่วนประกอบระบบแยกแยะออกจากส่วนกลางผ่าน เครื่องบินคุ้มกัน การเข้าถึงเครื่องบินคุ้มกัน โดยเจ้าหน้าที่ปฏิบัติการภายในต้องได้รับการอนุมัติสิทธิ์ มีเฉพาะเจ้าหน้าที่ปฏิบัติการภายในของ Tencent Cloud บางส่วนเท่านั้นที่สามารถเข้าถึงได้ และการเข้าสู่ระบบเครื่องบินคุ้มกัน ต้องการการยืนยันตัวตนสองปัจจัยสำหรับข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมการเข้าถึง

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			โปรดดูเนื้อหาในข้อ "3.1, 3.2 การควบคุมการเข้าถึง" ของ "5.3 เอกสารแนบ 2" การบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ" ในคู่มือนี้ ในด้านการจัดการลิขสิทธิ์ซอฟต์แวร์ พนักงานสามารถดาวน์โหลดซอฟต์แวร์ที่บริษัทอนุญาตเท่านั้น อนุญาตให้ติดตั้งเฉพาะซอฟต์แวร์ที่ผ่านการทดสอบแล้วเท่านั้น และสามารถติดตั้ง เรียกใช้ หรืออัปเดตซอฟต์แวร์ได้ก็ต่อเมื่อได้รับอนุญาตและอนุมัติเท่านั้น สำหรับซอฟต์แวร์ที่จัดซื้อ Tencent Cloud กำหนดความเป็นเจ้าของทรัพย์สินทางปัญญาของซอฟต์แวร์ที่จัดซื้อ วิธีการให้สิทธิใช้งาน ระยะเวลาการให้สิทธิใช้งาน เป็นต้น ไว้ในสัญญา ข้อตกลง อย่างชัดเจน และจัดสรรและติดตั้งซอฟต์แวร์ตามจำนวนลิขสิทธิ์ซอฟต์แวร์ที่ซื้อ หน่วยงานที่เกี่ยวข้องบำรุงรักษารายการซอฟต์แวร์ที่ติดตั้งโดยได้รับอนุญาต เพื่อให้แน่ใจว่าซอฟต์แวร์ที่ติดตั้งทั้งหมดมีการบันทึกไว้ ในด้านความปลอดภัยของข้อมูล ผลิตภัณฑ์การจัดเก็บข้อมูลและฐานข้อมูลหลายรายการของ Tencent Cloud รองรับฟังก์ชันการเข้ารหัสข้อมูล โดยใช้อัลกอริธึมการเข้ารหัสที่ปลอดภัยและมีความแข็งแกร่งสูง และผสมรวม Key Management Service (KMS) เพื่อจัดการวงจรชีวิตของคีย์อย่างครบถ้วน รับประกันความเป็นความลับของข้อมูล การสื่อสารของลูกค้าบนคอนโซล Tencent Cloud ได้รับการปกป้องด้วยการเข้ารหัสของโปรโตคอลความปลอดภัย HTTPS อินเทอร์เฟซ Cloud API ที่บริการผลิตภัณฑ์คลาวด์ของ Tencent Cloud ให้มั่นใจก็มีความสามารถด้านความปลอดภัย เช่น การเข้ารหัส HTTPS การตรวจสอบลายเซ็น และการตรวจสอบสถานะ เพื่อมอบความปลอดภัยในการสื่อสารระดับพอร์ตให้กับธุรกิจของลูกค้า สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการเทคโนโลยีการเข้ารหัส โปรดดูเนื้อหาในข้อ "6 การควบคุมการเข้ารหัส" ของ "11.3 ภาคผนวก 3" การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			ในด้านการจัดการวงจรชีวิตการพัฒนาระบบความปลอดภัย Tencent Cloud ยังได้สร้างมาตรฐานการพัฒนาความปลอดภัยระบบสารสนเทศภายในองค์กร และมุ่งมั่นพัฒนาตามมาตรฐาน ISO/IEC 20000 การจัดการบริการเทคโนโลยีสารสนเทศ ระบบการจัดการความปลอดภัยข้อมูล ISO/IEC 27001 และมาตรฐานระบบการจัดการคุณภาพ ISO/IEC 9001 เข้ากับกระบวนการวงจรชีวิตการพัฒนาความปลอดภัยผลิตภัณฑ์ทั้งหมด ให้มีความสำคัญกับขั้นตอนต่างๆ เช่น ความต้องการ การออกแบบ การวิจัยและพัฒนา การทดสอบ การส่งมอบ และการดำเนินการและบำรุงรักษา พยานแนวคิดด้านความปลอดภัยข้อมูลและการปกป้องความเป็นส่วนตัวเข้าไปในแต่ละขั้นตอนของการพัฒนาผลิตภัณฑ์ เพื่อให้มั่นใจว่าผลิตภัณฑ์คลาวด์ได้รับความควบคุมด้านความปลอดภัยที่เพียงพอตลอดวงจรชีวิตของผลิตภัณฑ์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวงจรชีวิตการพัฒนาระบบ โปรดดูเนื้อหาในข้อ "22 การจัดหาและการพัฒนาระบบ" ของ "14.1 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้ ในด้านการจัดการแพตช์ Tencent Cloud จะระบุแพตช์ล่าสุด และดำเนินการทดสอบความปลอดภัยอย่างเพียงพอก่อนการติดตั้งแพตช์ เพื่อให้มั่นใจในความปลอดภัยของการติดตั้งแพตช์ Tencent Cloud จะแจ้งให้ทีมงานธุรกิจภายในแต่ละทีมทราบเป็นประจำเกี่ยวกับการอัปเดตและติดตั้งแพตช์ และใช้เครื่องมือตรวจจับจุดปลายทาง (endpoint) สแกนสถานะการติดตั้งแพตช์เป็นประจำ และอุปกรณ์ที่ไม่ได้ติดตั้งแพตช์เกินกำหนดเวลาจะถูกสร้างใบงานแจ้งเตือนโดยอัตโนมัติ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการช่องโหว่และแพตช์ โปรดดูเนื้อหาในข้อ "8.11 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่" ของ "11.3 ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ" ในคู่มือนี้ ในด้านการจัดการขั้นตอนการปฏิบัติงานความปลอดภัยเครือข่าย Tencent Cloud ได้กำหนดมาตรฐานการจัดการการดำเนินงานและบำรุงรักษา

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อเป็นแนวทางและข้อกำหนดสำหรับพฤติกรรมกาปฏิบัติงานประจำวันของเจ้าหน้าที่ปฏิบัติการและบำรุงรักษา Tencent Cloud ใช้แพลตฟอร์มการจัดการการดำเนินงานและบำรุงรักษาแบบอัตโนมัติและเครื่องมือที่ครบครันเพื่อจัดการการดำเนินงานต่างๆ ควบคุมรอบเวลาการเปลี่ยนแปลงอย่างเคร่งครัดผ่านกลไกการจัดการภายใน เพื่อให้แน่ใจว่าคำขอการปฏิบัติงานทั้งหมดเสร็จสิ้นภายในเวลาที่กำหนด Tencent Cloud ยังกำหนด "เส้นแดง" ด้านความปลอดภัยในการปฏิบัติงานโดยละเอียด และดำเนินการตรวจสอบความปลอดภัยในการปฏิบัติงานภายในเป็นประจำ เพื่อให้มั่นใจว่าการดำเนินการในสภาพแวดล้อมการผลิตสามารถถูกควบคุมและติดตามได้ บันทึกการดำเนินงานแบ็กเอนด์ทั้งหมดจะถูกบันทึกโดยละเอียดและจัดเก็บบนแพลตฟอร์มบันทึกจากส่วนกลาง ทีมตรวจสอบภายในของ Tencent Cloud จะตรวจสอบและติดตามการดำเนินการที่น่าสงสัยในกระบวนการปฏิบัติงานเป็นประจำ ในด้านการรวบรวมและการวิเคราะห์ข้อมูลภัยคุกคามความปลอดภัยเครือข่าย เพื่อสนับสนุนลูกค้าในการตรวจจับและวิเคราะห์ภัยคุกคาม Tencent Cloud ให้บริการ Threat Intelligence X (TIX) แก่ลูกค้า ซึ่งเป็นแพลตฟอร์มบริการข่าวกรองแบบครบวงจร TIX สามารถให้ความสามารถด้านข่าวกรองสามประเภทหลัก ได้แก่ ข่าวกรองพื้นฐาน ข่าวกรองด้านพื้นผิวการโจมตี และข่าวกรองทางธุรกิจ รองรับฟังก์ชันต่างๆ เช่น การสืบค้นข่าวกรอง การวิเคราะห์และประเมิน IOC การจัดการพื้นผิวการโจมตี สามารถช่วยลูกค้าวิเคราะห์และประเมินเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น และประเมินความเสี่ยงด้านการเปิดเผยสินทรัพย์ขององค์กรอย่างครอบคลุมมากขึ้น สนับสนุนองค์กรในการสร้างระบบป้องกันความปลอดภัยแบบสามมิติที่มีประสิทธิภาพ TIX สร้างเครือข่ายจุดสัมผัสข่าวกรองที่สมบูรณ์ โดยรวบรวมและวิเคราะห์ข่าวกรองภัยคุกคามจากแหล่งที่มาหลากหลาย เช่น ชุมชนช่องโหว่ องค์กรความปลอดภัย ผู้ผลิตเครื่องมือความปลอดภัย โซเชียลมีเดีย บล็อกความปลอดภัย

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			และเชื่อมโยงกับอัลกอริทึมและพลังการคำนวณบนคลาวด์เพื่อ จัดผลบวกปลอม ซึ่งรับประกันความแม่นยำของชาวกรอง ด้วยการเสริมพลังและการสนับสนุนจากศูนย์ชาวกรองภัยคุ คาม Tencent Cloud มุ่งมั่นที่จะสร้างระบบความสามารถด้านความปลอดภัยในการ ป้องกันเชิงรุกแบบ "ชาวกรอง-การโจมตีและการป้องกัน- การจัดการ-การวางแผน" โดยบูรณาการเทคโนโลยีต่างๆ เช่น ชาวกรองภัยคุกคาม ปัญญาประดิษฐ์ ข้อมูลขนาดใหญ่ เพื่อเพิ่มความสามารถและประสิทธิภาพในการตอบสนองต่อเห ตุการณ์ความปลอดภัย และได้จัดตั้งศูนย์ปฏิบัติการความปลอดภัยที่ทำงาน 24 ชั่วโมงทุกวัน ให้ความสำคัญกับการตรวจจับภัยคุกคาม การสอบสวน และการตอบสนอง เพื่อให้บรรลุความสามารถในการรับรู้ มองเห็น และควบคุมสถานการณ์ความปลอดภัย
39	การตรวจจับแ ละการตรวจสอบ ภัยคุกคาม เครือข่าย	บริษัทต้องมีการตรวจสอบและเ ฝ้าระวังภัยคุกคามทางไซเบอร์ (detection) โดยจะต้องมีการดำเนินการอย่า งน้อย ดังต่อไปนี้ (๑) จัดให้มีช่องทางในการรายงาน ช่องโหว่ จุดอ่อน เหตุการณ์ หรือสถานการณ์ที่เกี่ยวข้อง ๗ ด้านความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดขอบเขตหน้าที่ควา มรับผิดชอบของหน่วยงานที่เกี่ ยวข้องทั้ง หน่วยงานภายในและหน่วยงาน ภายนอก (๒) กำหนดแนวทางในการค้นห า ทดสอบ และบริหารจัดการช่องโหว่ทางด้ านเทคโนโลยี สารสนเทศ เพื่อให้สามารถตรวจจับ วิเคราะห์ ติดตาม และแจ้งเตือนเหตุการณ์ผิดปกติ หรือภัยคุกคาม ทางไซเบอร์ให้แก่หน่วยงานหรือ ผู้รับผิดชอบรับทราบ	ลูกค้าควรเฝ้าระวังและตรวจจับภัยคุกคามหรือพฤติกรรมการ เข้าถึงโดยไม่ได้รับอนุญาตต่อระบบเทคโนโลยีสารสนเทศ และประเมินและซ่อมแซมช่องโหว่ของระบบเป็นประจำ โดยเฉพาะอย่างยิ่งสำหรับระบบที่มีความเสี่ยงสูง ควรดำเนินการทดสอบเจาะระบบ (penetration testing) เพื่อตรวจสอบประสิทธิภาพของเทคโนโลยีความปลอดภัย ในด้านการตรวจจับภัยคุกคาม เพื่อสนับสนุนลูกค้าในการตรวจจับและวิเคราะห์ภัยคุกคาม Tencent Cloud ให้บริการ Threat Intelligence X (TIX) แก่ลูกค้า ซึ่งเป็นแพลตฟอร์มบริการชาวกรองแบบครบวงจร TIX สามารถให้ความสามารถด้านชาวกรองสามประเภทหลัก ได้แก่ ชาวกรองพื้นฐาน ชาวกรองด้านพื้นผิวการโจมตี และชาวกรองทางธุรกิจ รองรับฟังก์ชันต่างๆ เช่น การสืบค้นชาวกรอง การวิเคราะห์และประเมิน IOC การจัดการพื้นผิวการโจมตี สามารถช่วยลูกค้าวิเคราะห์และประเมินเหตุการณ์ความปลอด ภัยได้อย่างมีประสิทธิภาพมากขึ้น และประเมินความเสี่ยงด้านการเปิดเผยสินทรัพย์ขององค์กรอ ย่างครอบคลุมมากขึ้น สนับสนุนองค์กรในการสร้างระบบป้องกันความปลอดภัยแบบ สามมิติที่มีประสิทธิภาพ ในด้านการทดสอบเจาะระบบ Tencent Cloud ให้บริการ Penetration Testing Service (PTS) แก่ลูกค้า ด้วยการจำลองเทคนิคการโจมตีและเทคนิคการค้นพบช่องโหว่

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		และกำหนดแนวทางในการสื่อสารและการดำเนินการแก้ไขในเบื้องต้นได้อย่างทันการณ์	ที่แอสเคอร์อาจใช้อย่างเต็มรูปแบบ ใช้วิธีการและกลไกที่ควบคุมได้และไม่ทำลายล้างเพื่อทำการตรวจสอบความปลอดภัยของระบบเป้าหมายอย่างลึกซึ้ง ค้นหาจุดอ่อนที่มีอยู่ในเป้าหมายและอุปกรณ์เครือข่าย ให้คำแนะนำในการเสริมความแข็งแกร่งด้านความปลอดภัยเพื่อช่วยลูกค้ายกระดับความปลอดภัยของระบบ และสนับสนุนการตรวจสอบหลังการแก้ไขช่องโหว่ ในด้านการสแกนช่องโหว่ ลูกค้าสามารถเลือกใช้ <u>Vulnerability Scanning Service (VSS)</u> เพื่อตรวจสอบสินทรัพย์เครือข่ายขององค์กรและระบุความเสี่ยงของสินทรัพย์นั้นๆ โดยใช้ประโยชน์จากประสบการณ์ด้านความปลอดภัยและข่าวกรองภัยคุกคามที่สะสมมาหลายปีของ Tencent Cloud VSS ได้สร้างฐานข้อมูลกฎช่องโหว่ที่อุดมสมบูรณ์และครอบคลุม และมีความสามารถในการตรวจจับช่องโหว่ 0Day/1Day/NDay ที่มีอาชีพและมีประสิทธิภาพสูง สามารถดำเนินการสแกนความปลอดภัยเป็นประจำ การแจ้งเตือนความเสี่ยงอย่างต่อเนื่อง และการตรวจจับช่องโหว่สำหรับความพร้อมใช้งาน ความปลอดภัย และความสอดคล้องของสินทรัพย์ของลูกค้า ให้คำแนะนำการแก้ไขที่มีอาชีพแก่ลูกค้า เพื่อลดความเสี่ยงด้านความปลอดภัย VSS ยังสนับสนุนการทำงานร่วมกับผลิตภัณฑ์คลาวด์ เช่น ความปลอดภัยโฮสต์ ไฟร์วอลล์แอปพลิเคชันเว็บ เพื่อให้บรรลุวงจรปิดจากการตรวจสอบความเสี่ยงไปจนถึงการจัดการความเสี่ยง เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล Tencent Cloud จะสร้างงานสแกนเป็นประจำผ่านระบบสแกนช่องโหว่เพื่อสแกนช่องโหว่ของสินทรัพย์ในสภาพแวดล้อมคลาวด์ และวิเคราะห์จัดประเภท และดำเนินการแก้ไขช่องโหว่ที่พบ ทีมงานด้านความปลอดภัยของ Tencent Cloud จะดำเนินการทดสอบเจาะระบบขนาดใหญ่แบบเต็มวงจรเป็นประจำ และดำเนินการทดสอบเจาะระบบแบบเจาะจงอย่างยืดหยุ่นในสถานการณ์ต่างๆ เช่น ก่อนการเปิดตัวผลิตภัณฑ์ใหม่หรือเมื่อมีการเปลี่ยนแปลงครั้งสำคัญ ผลการทดสอบเจาะระบบจะแจ้งให้ฝ่ายงานผู้รับผิดชอบที่เกี่ยวข้องทราบผ่านใบงานความปลอดภัย และฝ่ายงานผู้รับผิดชอบจะดำเนินการปะช่องโหว่หรือดำเนินการ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			าตรการควบคุมชุดอื่นๆ ทั้งนี้ เพื่อให้มั่นใจว่าช่องโหว่ที่ใช้ประโยชน์ได้ซึ่งพบในการทดสอบเจ าระบบได้รับการจัดการอย่างเหมาะสม นอกจากนี้ Tencent Cloud ยังดำเนินการฝึกซ้อมการต่อสู้เสมือนระหว่างทีมแดงและทีม น้ำเงินเพื่อจำลองการต้านทานการโจมตีทางเครือข่ายเป็นประ จำ Tencent Cloud ยังได้สร้างแพลตฟอร์มรับข้อเสนอแนะช่องโหว่จากภายนอกแ ละดำเนิน "โครงการให้รางวัลการรายงานช่องโหว่" โดยเชิญผู้เชี่ยวชาญด้านความปลอดภัยในอุตสาหกรรมช่วย Tencent Cloud ค้นพบช่องโหว่และความเสี่ยงด้านความปลอดภัยของระบบจา กมุมมองของแฮกเกอร์ เพื่อแก้ไขปัญหาด้านความปลอดภัยได้ทันเวลาที่ และบำรุงรักษาความปลอดภัยของระบบนิเวศของ Tencent Cloud สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการการตรวจจับและการ ตรวจสอบภัยคุกคาม โปรดดูเนื้อหาในข้อ "3.2 การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระ บบสารสนเทศ" ของ "10.2.3 <u>การรักษาความปลอดภัยพร้อมใช้งานของการให้บริการ</u> ในคู่มือนี้
40	การจัดการแล ะการตอบสน องต่อภัยคุคค าม	บริษัทต้องมีมาตรการในการรับ มือและตอบสนองเมื่อตรวจพบภ ยคุกคามทาง ไซเบอร์ (response) โดยจะต้องมีการดำเนินการอย่า งน้อย ดังต่อไปนี้ (๑) กำหนดแนวทางในการบริหาร จัดการการรับมือเหตุการณ์ผิ ดปกติหรือภัยคุกคามทาง ไซเบอร์ เพื่อให้บริษัทสามารถตอบสนอง และรับมือกับความเสี่ยงได้อย่าง ทันการณ์ (๒) กำหนดให้มีการจัดทำ ซักซ้อม หรือทดสอบแผนรับมือภัยคุคค ามทางไซเบอร์	ลูกค้าควรจัดทำมาตรการจัดการและตอบสนองสำหรับภัยคุคค คามความปลอดภัยทางไซเบอร์ที่ตรวจพบแล้ว จัดทำแนวทางในการจัดการและแก้ไขเหตุการณ์ผิดปกติหรือ ภัยคุกคาม ทดสอบและฝึกซ้อมแผนการตอบสนองต่อเหตุการณ์ความปล อดภัยทางไซเบอร์หรือแผนฉุกเฉินเป็นประจำ และจัดทำแผนการสื่อสารเพื่อให้มั่นใจว่าสามารถติดต่อผู้ที่เกี่ วข้องได้ทันเวลาที่เมื่อเกิดเหตุการณ์ เพื่อสนับสนุนให้ลูกค้าปฏิบัติตามข้อกำหนดทางการกำกับดูแล ล ในด้านการจัดการและตอบสนองต่อเหตุการณ์หรือภัย คุกคามความปลอดภัย Tencent Cloud ได้กำหนดมาตรฐานการจัดการเหตุการณ์ความปลอดภัยข้อ มูลภายในองค์กร สร้างกลไกและขั้นตอนที่เกี่ยวข้องสำหรับการรายงาน การตอบสนอง และการจัดการเหตุการณ์ความปลอดภัยข้อมูล Tencent

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		(cybersecurity) แผนฉุกเฉิน การสืบสวน และวิเคราะห์สาเหตุการแก้ปัญหา และจัดทำรายงานเพื่อ เสนอต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบ หมาย ๑๘	Cloud ใช้ระบบการดำเนินงานความปลอดภัยภายในเพื่อบันทึกเหตุการ ณ์ความปลอดภัย สำหรับเหตุการณ์ความปลอดภัยที่ตรวจจับและระบุได้ Tencent Cloud จะวิเคราะห์และจำแนกระดับเหตุการณ์โดยพิจารณาจากปัจเจก ยต่างๆ เช่น ลักษณะของเหตุการณ์
	(๓) กำหนดแนวทางในการสื่อสาร เพื่อดำเนินการแก้ไขเหตุการณ์หรือสถานการณ์จาก ภัยคุกคามทางไซเบอร์	ระดับความอ่อนไหวของข้อมูล และขอบเขตของผลกระทบ และจะแจ้งให้ผู้รับผิดชอบที่เกี่ยวข้องทราบทันทีเพื่อดำเนินการ จัดการเหตุการณ์ ในเวลาเดียวกัน Tencent Cloud มุ่งมั่นที่จะสร้างระบบความสามารถด้านความปลอดภัยในการ ป้องกันเชิงรุกแบบ "ข่าวกรอง-การโจมตีและการป้องกัน- การจัดการ-การวางแผน" โดยบูรณาการเทคโนโลยีต่างๆ เช่น ข่าวกรองภัยคุกคาม ปัญญาประดิษฐ์ ข้อมูลขนาดใหญ่ เพื่อเพิ่มความสามารถและประสิทธิภาพในการตอบสนองต่อเหตุ การณ์ความปลอดภัย ทีมงานของ Tencent Cloud มุ่งเน้นการตอบสนองไปที่การค้นพบช่องโหว่ การตรวจสอบการบุกรุก การป้องกันการโจมตี ฯลฯ ดำเนินการความปลอดภัยมืออาชีพ 24 ชั่วโมงทุกวัน สามารถเข้าแทรกแซงและจัดการการแจ้งเตือนความปลอดภัย ได้อย่างรวดเร็ว ดำเนินการวิเคราะห์เบื้องต้นและจัดทำแผนยับยั้ง เพื่อป้องกันการโจมตีหรือเหตุการณ์ความปลอดภัย ในระหว่างกระบวนการรับเรื่อง การสอบสวนและการประเมิน การจัดการ และการติดตาม ฝ่ายธุรกิจที่เกี่ยวข้องจะรับผิดชอบในการบำรุงรักษาระบบบันทึกขอ งเหตุการณ์ที่ได้รับไว้ และรับประกันความสมบูรณ์และความเป็นความลับของบันทึก	เพื่อสนับสนุนลูกค้าในการปฏิบัติหน้าที่ด้านการสื่อสาร และการแจ้งเตือนอย่างมีประสิทธิภาพ Tencent Cloud ได้กำหนดขั้นตอนการสื่อสารและการแจ้งเตือนเหตุการณ์ความ ปลอดภัยข้อมูล สร้างขั้นตอนที่เกี่ยวข้องสำหรับการแจ้งเตือนหรือการแจ้งให้พ นักงานภายในบริษัท ลูกค้า และผู้เกี่ยวข้องอื่นๆ ที่อาจหรือได้รับผลกระทบ เมื่อเกิดหรือกำลังจะเกิดอุบัติเหตุร้ายแรงหรือความขัดข้องทาง ธุรกิจที่สำคัญ เพื่อให้มั่นใจว่าทุกฝ่ายสามารถสื่อสารและประสานงานกันอย่าง เป็นระเบียบ ทันเวลา และมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบต่อ ลูกค้า Tencent Cloud

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้เหลือน้อยที่สุด ในด้านแผนฉุกเฉินสำหรับความปลอดภัยทางไซเบอร์ Tencent Cloud ได้สร้างแผนฉุกเฉินสำหรับความปลอดภัยทางไซเบอร์ซึ่งครอบคลุมสถานการณ์ฉุกเฉินด้านความปลอดภัยทางไซเบอร์หลายประเภท เช่น การโจมตีเครือข่าย โปรแกรมที่เป็นอันตราย ความปลอดภัยของข้อมูล ความล้มเหลวของอุปกรณ์และสิ่งอำนวยความสะดวก และเหตุการณ์ภัยพิบัติ โดยใช้การสร้างระบบแผนฉุกเฉินที่สมบูรณ์เป็นพื้นฐาน การสร้างทีมตอบสนองเหตุการณ์เป็นสนับสนุน และการกำหนดขั้นตอนการตอบสนองเหตุการณ์เป็นจุดเน้น เพื่อเพิ่มความสามารถในการตรวจสอบ การแจ้งเตือน การรายงาน และการจัดการ และป้องกันและลดผลกระทบด้านลบจากเหตุการณ์ความปลอดภัยทางไซเบอร์ต่อ Tencent Cloud หน่วยงานที่เกี่ยวข้องกับธุรกิจภายใน Tencent Cloud จะจัดฝึกอบรมและฝึกซ้อมแผนฉุกเฉินสำหรับเหตุการณ์ความปลอดภัยตามสถานการณ์เป็นประจำ และยังจัดฝึกอบรมทางเทคนิคให้กับพนักงานของทีมความปลอดภัยตามการพัฒนาของเทคโนโลยีความปลอดภัยและสถานการณ์ เพื่อให้มั่นใจว่าพนักงานเข้าใจและปฏิบัติตามข้อกำหนดและขั้นตอนการดำเนินงานด้านความปลอดภัยล่าสุด เรียนรู้มาตรฐานและแนวปฏิบัติที่ดีที่สุดด้านความปลอดภัยข้อมูลล่าสุด และสามารถตอบสนองต่อเหตุการณ์ความปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพ
41	การกู้คืนหลังความเสียหาย	บริษัทต้องมีแนวทางเพื่อฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (recovery) โดยจะต้องมีการดำเนินการอย่างน้อย ดังต่อไปนี้ (๑) กำหนดแนวทางและมาตรการในการฟื้นฟูความเสียหายจาก	ลูกค้าควรกำหนดแนวทางการกู้คืนและมาตรการตอบสนองให้ชัดเจนหลังเกิดความเสียหายจากภัยคุกคามความปลอดภัยทางไซเบอร์ และจัดทำแผนคำแนะนำการสื่อสารสำหรับงานกู้คืน เพื่อให้มั่นใจว่าลูกค้าสามารถตอบสนองและกู้คืนฟังก์ชันสำคัญได้อย่างรวดเร็วหลังเกิดเหตุการณ์ภัยพิบัติ ผลิตภัณฑ์/บริการคลาวด์ต่างๆ ที่ Tencent Cloud ให้มา

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
	เหตุการณ์ หรือ สถานการณ์จากภัยคุกคามทาง ไซเบอร์	เหตุการณ์ หรือ สถานการณ์จากภัยคุกคามทาง ไซเบอร์	เช่น บริการคอมพิวเตอร์ บริการเครือข่าย บริการจัดเก็บข้อมูล บริการฐานข้อมูล บริการคอนเทนเนอร์และมิดเดิลแวร์ บริการความปลอดภัย
	สอดคล้องกับผลการประเมินคว ามเสี่ยงและผลกระทบตามกรอ บ	สอดคล้องกับผลการประเมินคว ามเสี่ยงและผลกระทบตามกรอ บ	ล้วนมีคุณลักษณะความพร้อมใช้งานสูง และมีแผนการกู้คืนจากภัยพิบัติที่สอดคล้องกัน เช่น Cloud Virtual Machine (CVM)
	การดำเนินงานความมั่นคงปลอดภัยไซเบอร์และการบริหารจัดการ ความเสี่ยงด้านเทคโนโลยีสาร สนเทศ ของบริษัท	การดำเนินงานความมั่นคงปลอดภัยไซเบอร์และการบริหารจัดการ ความเสี่ยงด้านเทคโนโลยีสาร สนเทศ ของบริษัท	มีคุณลักษณะของความพร้อมใช้งานสูงของบริการและความน่า เชื่อถือสูงของข้อมูล Cloud Block Storage ที่ใช้กับ CVM ให้กลยุทธ์การจัดเก็บข้อมูลสำรองสามชุด ซึ่งรับประกันความสามารถในการย้ายและกู้คืนข้อมูลได้อย่าง รวดเร็วเมื่อสำเนาใดสำเนาหนึ่งขัดข้อง
	(๒) กำหนดแนวทางในการสื่อสาร เพื่อดำเนินการฟื้นฟูความเสี ยจากเหตุการณ์หรือ	(๒) กำหนดแนวทางในการสื่อสาร เพื่อดำเนินการฟื้นฟูความเสี ยจากเหตุการณ์หรือ	สำหรับการรับประกันความยืดหยุ่นของโครงสร้างพื้นฐาน และอุปกรณ์ ระบบไฟฟ้าและระบบปรับอากาศของศูนย์ข้อมูลทั่วโลกของ Tencent Cloud ล้วนใช้การออกแบบแบบซ้ำซ้อนเต็มรูปแบบที่มีความเสถียรสูง เพื่อหลีกเลี่ยงไม่ให้ความล้มเหลวของจุดใดจุดหนึ่งส่งผลกระทบต่อคว ามต่อเนื่องของไฟฟ้าและการระบายความร้อนของศูนย์ข้อมูล นอกจากนี้ เจ้าหน้าที่รักษาความปลอดภัยของศูนย์ข้อมูลแต่ละแห่งของ Tencent Cloud จะดำเนินการตรวจสอบสถานการณ์ของห้องเซิร์ฟเวอร์และอุป กรณ์ต่างๆ อย่างเคร่งครัดตามรายการตรวจสอบและแผนการตรวจสอบเ ป็นประจำ และจะลงนามและบันทึกเวลาตรวจสอบที่จุดตรวจแต่ละแห่ง เมื่อพบความขัดข้องของโครงสร้างพื้นฐานหรือเหตุการณ์ด้าน ความปลอดภัย จะเริ่มต้นขั้นตอนการตอบสนองเหตุการณ์ของศูนย์ข้อมูลทันที เพื่อรับประกันการดำเนินการขั้นตอนการกู้คืนที่รวดเร็วและมี ประสิทธิภาพ และสนับสนุนลูกค้าในการบรรลุการกู้คืนจากภัยพิบัติได้ทันท ่วงที่ Tencent Cloud ได้สร้างระบบการจัดการความต่อเนื่องของธุรกิจที่ครอบคลุม โดยกำหนดบทบาทของบุคลากรในกระบวนการกู้คืนธุรกิจเป็น หน่วยงาน และกำหนดหน้าที่และความรับผิดชอบในการแบ่งงานกันในการ กระบวนการกู้คืนให้ชัดเจน

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
42	การประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์	บริษัทต้องมีการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ (cybersecurity risk assessment) โดยการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามทางไซเบอร์ เพื่อให้ทราบถึงสถานภาพความเสี่ยงจากภัยคุกคามทางไซเบอร์ของบริษัทตามสภาพปัจจัยความเสี่ยง สถานการณ์ความเสี่ยง ภัยคุกคามหรือช่องโหว่ที่เกี่ยวข้องในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาปัจจัยความเสี่ยงจากภัยคุกคามทางไซเบอร์ ดังต่อไปนี้ (๑)เกณฑ์ในการประเมินและจัดระดับความรุนแรง และผลกระทบของเหตุการณ์ หรือ สถานการณ์การถูกโจมตีทางไซเบอร์ รวมทั้งโอกาสเกิดของเหตุการณ์ ตลอดจนการประเมินระดับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (๒)จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามทางไซเบอร์ และต้องมีรายงานผลการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ และ แนวโน้มของความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นต่อคณะกรรมการบริษัท หรือ คณะกรรมการชุดย่อยที่ได้รับมอบหมาย ในระยะเวลาที่เหมาะสม	ลูกค้าควรดำเนินการประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์เป็นประจำ เพื่อระบุความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์และภัยคุกคามเครือข่าย จัดระดับความเสี่ยงตามระดับความรุนแรง ระดับผลกระทบ และความเป็นไปได้ที่จะเกิดขึ้น และรายงานผลการประเมินความเสี่ยงและแนวโน้มต่อฝ่ายบริหาร Tencent Cloud ได้กำหนดขั้นตอนการจัดการความเสี่ยงด้านความปลอดภัยข้อมูลภายในองค์กร ซึ่งกำหนดนิยามและให้คำแนะนำเกี่ยวกับเนื้อหาการทำงานของการจัดการความเสี่ยงทั้งหมด (การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง การกำหนดแผนการจัดการความเสี่ยง และการติดตามและตรวจสอบความเสี่ยง) ไว้อย่างชัดเจน การระบุความเสี่ยง: Tencent Cloud ดำเนินการประเมินความเสี่ยงเป็นประจำ โดยระบุสถานการณ์ความเสี่ยงที่ใช้ได้กับ Tencent Cloud จากแหล่งต่างๆ เช่น รายงานเหตุการณ์ความปลอดภัยในอุตสาหกรรม การสะสมประสบการณ์การปฏิบัติของ Tencent Cloud ฐานข้อมูลความเสี่ยงของสถาบันมืออาชีพ และระบุความเสี่ยงตามผลการวิเคราะห์กระบวนการของ สถานการณ์ความเสี่ยง ผลิตภัณฑ์หรือบริการทางธุรกิจ การประเมินความเสี่ยง: Tencent Cloud ประเมินมูลค่าสินทรัพย์ ความเป็นไปได้ของความเสี่ยงในสถานการณ์ความเสี่ยง และระดับผลกระทบของความเสี่ยง และคำนวณระดับความเสี่ยง การจัดการความเสี่ยง: ตามผลการวิเคราะห์ความเสี่ยง สำหรับความเสี่ยงที่ระบุ Tencent Cloud จะใช้กลยุทธ์การตอบสนองและมาตรการบรรเทาความเสี่ยงที่สอดคล้องกัน สำหรับความเสี่ยงสูง ผู้รับผิดชอบด้านความเสี่ยงจะจัดทำแผนจัดการความเสี่ยง (มาตรการการโอนย้ายหรือลดความเสี่ยง) และอัปเดตตารางการจัดการความเสี่ยง สำหรับความเสี่ยงปานกลาง ผู้รับผิดชอบด้านความเสี่ยงจะตัดสินใจตามสภาพแวดล้อม

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			จริงว่าจำเป็นต้องจัดทำแผนจัดการความเสี่ยงหรือไม่ สำหรับความเสี่ยงต่ำถือเป็นความเสี่ยงที่ยอมรับได้ สำหรับความเสี่ยงที่เหลือ Tencent Cloud จะทบทวนทุกครั้ง เพื่อตรวจสอบสถานะและมูลค่าความเสี่ยง การติดตาม การทบทวน และการรายงานความเสี่ยง: Tencent Cloud รวมผลการประเมินความเสี่ยง ออกรายงานการประเมินความเสี่ยง และรายงานต่อฝ่ายบริหาร และบำรุงรักษาตารางการจัดการความเสี่ยง ติดตามการเปลี่ยนแปลงเงื่อนไขความเสี่ยงและสถานะของ แผนจัดการความเสี่ยง และปรับแผนการจัดการความเสี่ยงแบบเรียลไทม์ นอกจากนี้ Tencent Cloud ยังกำหนดตัวชี้วัดความเสี่ยงที่สำคัญและวัดตัวชี้วัดความเสี่ยง ที่สำคัญเป็นประจำ เทียบเคียงกับเกณฑ์ความเสี่ยงที่ยอมรับได้ วิเคราะห์สาเหตุรากฐานของปัญหาที่พบ และเสนอข้อเสนอแนะและแนวทางในการปรับปรุง

14.6

การรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์หรือภัยคุกคามที่มีต่อระบบเทคโนโลยีสารสนเทศ

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
43	การรายงานภัย คุกคามความ ปลอดภัยทาง ไซเบอร์	บริษัทต้องมีการรายงานเหตุการณ์ภัย คุกคามทางไซเบอร์หรือภัยคุกคาม ที่มีต่อระบบเทคโนโลยีสารสนเทศ ดังต่อไปนี้ (๑) รายงานต่อสำนักงานในกรณีที่เกิ ดปัญหาหรือเหตุการณ์ที่มีนัยสำคัญ ในการใช้ เทคโนโลยีสารสนเทศซึ่งส่งผลกระทบ ต่อการให้บริการ หรือระบบ หรือข้อมูลผู้เอาประกันภัย หรือ ชื่อเสียงของบริษัท และให้รวมถึงกรณีที่เทคโนโลยีสารสนเทศ	เมื่อลูกค้าเกิดหรือพบปัญหาใหญ่หรือเหตุการณ์ที่เกี่ยวข้อง กับการประยุกต์ใช้เทคโนโลยีสารสนเทศ ควรรายงานต่อฝ่ายบริหารทันที และรายงานต่อคณะกรรมการประกันภัย หากเกิดการโจมตีจากภัยคุกคามเครือข่าย ทำให้บริการโครงสร้างพื้นฐานข้อมูลสำคัญของบริษัทขัด ข้องหรือเกิดเหตุการณ์ ควรรายงานต่อคณะกรรมการประกันภัยภายใน 72 ชั่วโมง และดำเนินการตอบสนองและจัดการ เพื่อสนับสนุนลูกค้าในการตรวจจับและวิเคราะห์ภัย คุกคาม Tencent Cloud ให้บริการ Threat Intelligence X (TIX) แก่ลูกค้า

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
		นเทศที่สำคัญของบริษัทถูกโจมตีหรือถูกขโมย จากภัยคุกคามทางไซเบอร์และเป็นปัญหาหรือเหตุการณ์ที่บริษัทต้องรายงานต่อผู้บริหารสูงสุดของบริษัททราบ ให้บริษัทรายงานต่อสำนักงานทันทีเมื่อเกิดหรือรับรู้เหตุการณ์นั้น พร้อมแจ้งรายละเอียด และสาเหตุของเหตุการณ์ที่เกิดขึ้น ผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไข ปัญหา ระยะเวลาในการแก้ไข และแนวทางป้องกันในอนาคต (๒)กรณีที่บริษัทถูกโจมตีจากภัยคุกคามทางไซเบอร์ เป็นปัญหาหรือเหตุการณ์ที่เกี่ยวข้อง กับการให้บริการโครงสร้างพื้นฐาน สำคัญทางสารสนเทศที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ต้องแจ้งเหตุการณ์ ละเมิดโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงไปยังสำนักงานหรือหน่วยงานตามที่กฎหมายกำหนด รวมถึง การให้ข้อมูลหรือประสานกับหน่วยงานของรัฐ หรือหน่วยงานองค์กรที่แต่งตั้งขึ้นตามกฎหมายว่าด้วย การรักษาความมั่นคงปลอดภัยไซเบอร์ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์	ซึ่งเป็นแพลตฟอร์มบริการเช่าครองแบบครบวงจร TIX สามารถให้ความสามารถด้านเช่าครองสามประเภทหลักได้แก่ เช่าครองพื้นฐาน เช่าครองด้านพื้นผิวการโจมตี และเช่าครองทางธุรกิจ รองรับฟังก์ชันต่างๆ เช่น การสืบค้นเช่าครอง การวิเคราะห์และประเมิน IOC การจัดการพื้นผิวการโจมตี สามารถช่วยลูกค้าวิเคราะห์และประเมินเหตุการณ์ความปลอดภัยได้อย่างมีประสิทธิภาพมากขึ้น และประเมินความเสี่ยงด้านการเปิดเผยสินทรัพย์ขององค์กรอย่างครอบคลุมมากขึ้น สนับสนุนองค์กรในการสร้างระบบป้องกันความปลอดภัยแบบสามมิติที่มีประสิทธิภาพ TIX สร้างเครือข่ายจุดสัมผัสเช่าครองที่สมบูรณ์ โดยรวบรวมและวิเคราะห์เช่าครองภัยคุกคามจากแหล่งที่มาหลากหลาย เช่น ชุมชนช่องโหว่ องค์กรความปลอดภัย ผู้ผลิตเครื่องมือความปลอดภัย โซเชี่ยลมีเดีย บล็อกความปลอดภัย และเชื่อมโยงกับอัลกอริธึมและพลังการคำนวณบนคลาวด์ เพื่อจัดผลบวกปลอม ซึ่งรับประกันความแม่นยำของเช่าครอง ด้วยการเสริมพลังและการสนับสนุนจากศูนย์เช่าครองภัยคุกคาม Tencent Cloud มุ่งมั่นที่จะสร้างระบบความสามารถด้านความปลอดภัยในการป้องกันเชิงรุกแบบ "เช่าครอง-การโจมตีและการป้องกัน-การจัดการ-การวางแผน" โดยบูรณาการเทคโนโลยีต่างๆ เช่น เช่าครองภัยคุกคาม ปัญญาประดิษฐ์ ข้อมูลขนาดใหญ่ เพื่อเพิ่มความสามารถและประสิทธิภาพในการตอบสนองต่อเหตุการณ์ความปลอดภัย และได้จัดตั้งศูนย์ปฏิบัติการความปลอดภัยที่ทำงาน 24 ชั่วโมงทุกวัน ให้มีความสำคัญกับการตรวจจับภัยคุกคาม การสอบสวน และการตอบสนอง เพื่อให้บรรลุความสามารถในการรับรู้มองเห็น และควบคุมสถานการณ์ความปลอดภัย เพื่อสนับสนุนลูกค้าในการปฏิบัติหน้าที่ด้านการสื่อสารและการแจ้งเตือนอย่างมีประสิทธิภาพ Tencent Cloud ได้กำหนดมาตรฐานการจัดการเหตุการณ์ความปลอดภัยข้อมูล สร้างขั้นตอนที่เกี่ยวข้อง เช่น การตอบสนองเหตุการณ์ความปลอดภัยข้อมูล การยกระดับเหตุการณ์ และการแจ้งเหตุการณ์

ลำดับ ที่	โดเมนการ ควบคุม	ข้อกำหนดควบคุมเฉพาะ	การตอบสนองของ Tencent Cloud
			เพื่อแจ้งเตือนหรือแจ้งให้พนักงานภายในบริษัท ลูกค้าและผู้เกี่ยวข้องอื่น ๆ ที่อาจหรือได้รับผลกระทบจากอุบัติเหตุทราบทันเวลา ทำให้ทุกฝ่ายสามารถสื่อสารและประสานงานกันอย่างเป็นระเบียบ ทันเวลา และมีประสิทธิภาพ สำหรับเหตุการณ์ความปลอดภัยที่อาจส่งผลกระทบต่อลูกค้า Tencent Cloud จะพิจารณาขอบเขตและระดับผลกระทบของเหตุการณ์ความปลอดภัยข้อมูล และหลังจากผ่านการทบทวนภายในแล้ว จะแจ้งผลการจัดการและวิเคราะห์เหตุการณ์ความปลอดภัยข้อมูลให้ลูกค้าทราบผ่านช่องทางที่เหมาะสม และให้การสนับสนุนทางเทคนิคที่สอดคล้องกัน เพื่อช่วยลูกค้าใช้มาตรการแก้ไขเพื่อลดความสูญเสียให้เหลือน้อยที่สุด

15

ส่วนท้าย

Tencent Cloud เป็นแบรนด์คอมพิวเตอร์คลาวด์ที่ Tencent Group สร้างขึ้นด้วยความอุตสาหะ ซึ่งต่อยอดประสบการณ์ทางเทคนิคและความสามารถด้านความปลอดภัยที่ Tencent ส่งสมมาหลายปี Tencent Cloud มุ่งมั่นที่จะให้บริการคลาวด์ที่ปลอดภัย น่าเชื่อถือ และชาญฉลาดแก่ลูกค้าอย่างต่อเนื่อง เพื่อช่วยเหลือธุรกิจจำนวนมากขึ้นในการเผชิญหน้ากับคลื่นดิจิทัลอย่างมีประสิทธิภาพ และส่งเสริมการพัฒนายอย่างปลอดภัยขององค์กร

คู่มือนี้ได้อ้างอิงข้อกำหนดด้านกฎระเบียบที่สำคัญจากธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เพื่อแสดงให้ลูกค้าเห็นอย่างครอบคลุมและโปร่งใสว่า Tencent Cloud สามารถช่วยลูกค้าให้ระบบและข้อมูลบนคลาวด์เป็นไปตามข้อกำหนดได้อย่างไร และช่วยลูกค้าธุรกิจให้วางใจและอุ่นใจในการโฮสต์ระบบและข้อมูลบนคลาวด์ Tencent Cloud หวังว่าคู่มือนี้จะสนับสนุนลูกค้าธุรกิจในการปฏิบัติตามมาตรฐานการปฏิบัติตามข้อกำหนดทางกฎระเบียบทางการเงินของประเทศไทยอย่างมีประสิทธิภาพ

ขณะเดียวกันก็บรรเทาการอัปเดตดิจิทัลและการพัฒนานวัตกรรมทางธุรกิจอย่างมีประสิทธิภาพ

คู่มือนี้จัดทำขึ้นเพื่อวัตถุประสงค์ในการอ้างอิงเท่านั้น สำหรับข้อมูลในคู่มือนี้ ลูกค้าสามารถใช้ตามความเหมาะสมตามสถานการณ์จริงของตนเอง เพื่อให้มั่นใจในความสอดคล้องตามกฎระเบียบในระหว่างกระบวนการใช้บริการคลาวด์ของ Tencent Cloud

16

ประวัติเวอร์ชัน

วันที่	เวอร์ชัน	รายละเอียด
เมษายน 2569	V1.0	การปล่อยครั้งแรก