



Panduan Kepatuhan Tencent Cloud terhadap Persyaratan Regulasi Industri Keuangan Indonesia

April 2026

【Pernyataan Hak Cipta】

©2013-2026 Tencent Cloud Seluruh hak cipta dilindungi undang-undang

Dokumen ini adalah hak cipta eksklusif Tencent Cloud. Tanpa izin tertulis sebelumnya dari Tencent Cloud, tidak ada pihak yang diizinkan untuk memperbanyak, memodifikasi, menyalin, atau menyebarkan seluruh atau sebagian isi dokumen ini dalam bentuk apa pun.

【Pernyataan Merek Dagang】



serta merek dagang lain yang terkait dengan layanan Tencent Cloud adalah hak milik Tencent Computing (Beijing) Co., Ltd. dan perusahaan afiliasinya. Merek dagang pihak ketiga yang disebutkan dalam dokumen ini adalah hak milik pemegangnya sesuai hukum yang berlaku.

【Pernyataan Layanan】

Dokumen ini disediakan hanya sebagai referensi. Tencent Cloud tidak memberikan jaminan apa pun, baik tersurat maupun tersirat, terkait informasi dalam dokumen ini. Dokumen ini disusun berdasarkan kondisi saat ini.

Informasi dan referensi yang tercantum di sini, termasuk tautan ke situs web pihak ketiga, dapat berubah tanpa pemberitahuan sebelumnya. Penggunaan dokumen ini sepenuhnya menjadi tanggung jawab dan risiko pengguna.

Dokumen ini tidak memberikan hak hukum atas kekayaan intelektual produk Tencent apa pun kepada pengguna. Anda diperbolehkan memperbanyak dan menggunakan konten dokumen ini hanya untuk keperluan referensi internal.

Contoh-contoh yang dijelaskan di sini hanya bersifat ilustratif dan bersifat fiktif. Tidak boleh disimpulkan atau diharapkan adanya hubungan atau kaitan faktual berdasarkan contoh-contoh tersebut.

CONTENTS

01	Ringkasan	
02	Keamanan dan Kepatuhan Privasi Tencent Cloud	
	2.1 Sertifikasi Otoritatif Internasional	5
	2.2 Sertifikasi Sistem ISO/IEC	6
	2.3 Sertifikasi Regional & Industri	9
03	Model Tanggung Jawab Bersama untuk Keamanan Cloud Tencent	
04	Infrastruktur Global Tencent Cloud	
05	Bagaimana Tencent Cloud Membantu Mematuhi dan Mendukung Pelanggan Dalam Memenuhi Persyaratan Manajemen Risiko Terkait Penggunaan Teknologi Informasi Perbankan Komersial	
	5.1 Manajemen Teknologi Informasi	28
	5.2 Langkah Pengendalian dalam Pengembangan dan Pengadaan	33
	5.3 Operasional Teknologi Informasi	44
	5.4 Teknologi Jaringan Komunikasi	82
	5.5 Pengamanan Informasi	93
	5.6 Rencana Pemulihan Bencana	119
	5.7 Audit Intern	131
	5.8 Penggunaan Pihak Penyedia Jasa TI	132
	5.9 Pelaporan	145
06	Bagaimana Tencent Cloud Mematuhi dan Membantu Pelanggan Memenuhi Peraturan Penerapan Teknologi Informasi untuk Bank Umum dan Lembaga Jasa Keuangan Non-Bank	
07	Bagaimana Tencent Cloud Mematuhi dan Membantu Pelanggan Memenuhi Tentang Ketahanan dan Keamanan Siber Bagi Bank Umum	
	7.1 Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber	193
	7.2 Penilaian Kualitas Penerapan Proses Ketahanan Siber	207
08	Penutup	
09	Riwayat Versi	

01 Ringkasan

The background features several overlapping, semi-transparent blue shapes. A large, light blue circle is positioned in the upper left. Below it, a series of overlapping, petal-like shapes in various shades of blue (from light to dark) form a stylized flower or star pattern in the lower right quadrant.

Otoritas Jasa Keuangan Indonesia (Financial Services Authority of Indonesia, selanjutnya disebut "OJK") sebagai regulator sektor jasa keuangan Indonesia, memiliki tanggung jawab inti untuk memastikan berjalannya sistem keuangan secara transparan, aman, dan efisien melalui pembangunan kerangka regulasi yang kuat serta penguatan pengawasan industri, guna menjaga stabilitas pasar keuangan dan kepercayaan publik. Seiring dengan mendalamnya transformasi digital global, berbagai lembaga keuangan di Indonesia secara aktif meningkatkan penerapan sistem elektronik, mengoptimalkan proses bisnis, serta meningkatkan efisiensi operasional dan kualitas layanan melalui pengenalan alat-alat digital. Dalam konteks ini, untuk mencegah risiko yang mungkin timbul dari penerapan teknologi informasi oleh lembaga keuangan dan mendukung transformasi digital keuangan yang berkelanjutan, OJK secara bertahap merumuskan dan menerbitkan sejumlah dokumen kebijakan yang bertujuan, memperjelas persyaratan manajemen risiko lembaga keuangan dalam penggunaan teknologi informasi, serta memberikan pedoman dan arahan regulasi yang jelas bagi lembaga keuangan untuk mengembangkan bisnis digital secara teratur dan memperkuat pencegahan serta pengendalian risiko.

Tencent Cloud memantau perkembangan dan publikasi terbaru dari Otoritas Jasa Keuangan Indonesia, dan berkomitmen untuk membantu lembaga keuangan Indonesia memenuhi persyaratan regulasi dari otoritas pengawas. Dokumen ini akan menjelaskan bagaimana Tencent Cloud membantu pelanggan mematuhi persyaratan regulasi, dengan fokus pada pedoman dan pemberitahuan pengawasan berikut yang menjadi perhatian utama pelanggan:

- [NOMOR 38 /POJK.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum](#)
- [NOMOR 13 /POJK.03/2020 Tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan NOMOR 38/POJK.03/2016](#)
- [NOMOR 21 /SEOJK.03/2017 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum](#)

- [NOMOR 11 /POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi](#)
- [NOMOR 4 /POJK.05/2021 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Lembaga Jasa Keuangan Nonbank](#)
- [NOMOR 29 /SEOJK.03/2022 Tentang Ketahanan dan Keamanan Siber Bagi Bank Umum](#)

02

Keamanan dan Kepatuhan Privasi Tencent Cloud

Kepatuhan adalah fondasi pengembangan Tencent Cloud. Tencent Cloud mengidentifikasi dan menerapkan standar keamanan internasional dan industri yang mutakhir, mematuhi persyaratan kepatuhan di berbagai negara/wilayah dan sektor, terus menyempurnakan sistem manajemen internal, meningkatkan tingkat kontrol keamanan Tencent Cloud, serta berupaya sepenuhnya membangun layanan cloud yang dapat dipercaya oleh pelanggan. Secara bersamaan, Tencent Cloud juga aktif berpartisipasi dalam perumusan dan promosi standar keamanan industri, berpegang pada prinsip kepatuhan sebagai layanan, serta membangun dan mengoperasikan ekosistem cloud yang aman dan andal.

Hingga saat ini, Tencent Cloud telah memperoleh berbagai sertifikasi dan kualifikasi kepatuhan keamanan serta privasi melalui audit atau penilaian independen pihak ketiga, membuktikan bahwa pembangunan manajemen keamanan dan perlindungan privasi Tencent Cloud memenuhi standar sertifikasi terkait atau praktik baik industri. Untuk informasi lebih lanjut tentang kepatuhan Tencent Cloud, silakan lihat halaman [Tencent Cloud Compliance Center](#). Jika memerlukan sertifikat atau laporan kepatuhan terkait, harap ajukan permohonan dan unduh melalui [Compliance Document Download](#).

Berikut adalah beberapa contoh sertifikasi otoritatif internasional, serta pengakuan regional dan industri dari Tencent Cloud:

2.1 Sertifikasi Otoritatif Internasional

Sertifikasi Keamanan Cloud	STAR (Security, Trust & Assurance Registry) adalah sertifikasi keamanan cloud internasional yang diluncurkan oleh Cloud Security Alliance (CSA), organisasi nirlaba otoritatif global.
CSA STAR	Sertifikasi ini memperluas kerangka Sistem Manajemen Keamanan Informasi ISO/IEC 27001 dengan mengintegrasikan Cloud Control Matrix (CCM), sehingga memvisualisasikan isu-isu spesifik keamanan cloud dan memberikan gambaran umum yang intuitif kepada pengguna mengenai evaluasi arsitektur keamanan.

Berdasarkan praktik keamanan yang telah terakumulasi oleh Tencent selama bertahun-tahun, Tencent Cloud telah meraih

sertifikasi CSA STAR Gold tingkat global. Pencapaian ini menunjukkan bahwa sistem pengendalian keamanan Tencent Cloud memenuhi standar keamanan cloud internasional yang diakui secara luas.

Audit SOC Laporan System and Organization Controls (selanjutnya disebut "Laporan SOC") adalah serangkaian laporan terkait kontrol internal penyedia layanan yang diterbitkan oleh kantor akuntan publik pihak ketiga profesional sesuai dengan standar yang ditetapkan oleh American Institute of Certified Public Accountants (AICPA). Sebagai laporan audit independen, Laporan SOC mencakup titik-titik kontrol yang berkaitan dengan keamanan, ketersediaan, dan kerahasiaan platform Tencent Cloud.

Berdasarkan jenis layanan asuransi yang berbeda, Laporan SOC dapat disediakan bagi pengguna cloud serta auditor mereka, memberikan informasi berharga kepada pengguna Tencent Cloud untuk mengevaluasi dan mengatasi risiko yang terkait dengan penyedia layanan.

2.2 Sertifikasi Sistem ISO/IEC

Sertifikasi ISO/IEC 22301: 2019 ISO/IEC 22301: 2019 adalah standar internasional yang berfokus pada Manajemen Kelangsungan Bisnis (Business Continuity Management, BCM). Standar ini menyediakan metodologi BCM yang komprehensif dan universal, dengan tujuan membantu perusahaan mengidentifikasi dan merespons peristiwa-peristiwa disruptif potensial, memastikan kelangsungan operasi kritis, sehingga mengurangi risiko dan melindungi organisasi dari dampak signifikan.

Tencent Cloud telah memperoleh sertifikasi ISO/IEC 22301: 2019, yang membuktikan bahwa Tencent Cloud telah membangun proses manajemen kelangsungan bisnis yang formal untuk menjamin keberlanjutan dan stabilitas operasi bisnisnya sendiri.

Sertifikasi ISO/IEC 27001: 2022 ISO/IEC 27001: 2022 adalah standar sertifikasi Sistem Manajemen Keamanan Informasi (ISMS) yang paling diakui, ketat, dan diterima secara luas di tingkat internasional dalam bidang keamanan informasi. Dengan memperoleh sertifikasi ini, sebuah perusahaan

menunjukkan bahwa mereka telah membangun sistem manajemen keamanan informasi yang ilmiah dan efektif, guna menyelaraskan strategi pengembangan perusahaan dengan langkah-langkah manajemen keamanan informasi, serta memastikan risiko keamanan informasi yang relevan dikendalikan dan ditangani dengan tepat.

Sertifikasi ISO/IEC 27001: 2022 lebih mencerminkan komitmen Tencent Cloud terhadap keamanan, menunjukkan bahwa Tencent Cloud telah membangun sistem manajemen yang ilmiah dan efektif, serta mampu menyediakan produk dan layanan cloud yang aman dan dapat diandalkan bagi pengguna.

Sertifikasi ISO/IEC 20000-1: 2018 merupakan standar internasional yang dirumuskan khusus untuk manajemen layanan teknologi informasi (ITSM). Sistem ini menstandarisasi manajemen layanan TI suatu perusahaan, mencakup pola pembentukan, penerapan, operasi, pemantauan, peninjauan, pemeliharaan, dan peningkatan, guna membantu perusahaan secara berkelanjutan mengidentifikasi dan mengelola permasalahan TI terkait, memperkuat komunikasi dengan pengguna, serta membangun sistem layanan terstandar yang mampu menyempurnakan diri.

Tencent Cloud telah memperoleh sertifikasi ISO/IEC 20000-1: 2018 dengan cakupan sertifikasi yang meliputi layanan komputasi awan, layanan terkelola (managed services), serta layanan pemulihan bencana. Dengan pendekatan yang berorientasi pada layanan prima, Tencent Cloud secara konsisten menyempurnakan mekanisme layanan dan komunikasi teknologi informasi dengan pelanggan.

Sertifikasi ISO/IEC 9001: 2015 adalah sistem manajemen mutu yang matang dan diakui secara luas di tingkat internasional. Sistem ini menyediakan kerangka kerja dan pedoman normatif untuk manajemen mutu di seluruh proses penyediaan produk atau layanan perusahaan, bertujuan membantu perusahaan mempertahankan produk atau layanannya serta memastikan kualitas yang stabil dan konsisten dalam penyerahan.

Tencent Cloud telah memperoleh sertifikasi ISO/IEC 9001 dengan cakupan yang meliputi layanan komputasi awan, layanan terkelola,

serta layanan pemulihan bencana. Dengan menerapkan sistem manajemen mutu, Tencent Cloud mencapai target mutu yang diharapkan secara efektif dan efisien, sehingga menjamin kualitas produk dan layanan cloud serta operasionalnya.

Sertifikasi ISO/IEC 27017: 2015 ISO/IEC 27017: 2015 merupakan pelengkap dari ISO/IEC 27002: 2013 dan merupakan standar praktis untuk keamanan informasi layanan cloud. Standar ini menyediakan kontrol keamanan spesifik beserta panduan penerapannya bagi penyedia layanan cloud dan pelanggan, sehingga memperkuat pengendalian atas ancaman dan risiko kerentanan dalam komputasi awan.

Tencent Cloud telah memperoleh sertifikasi ISO/IEC 27017: 2015. Hal ini tidak hanya menunjukkan bahwa Tencent Cloud senantiasa mengadopsi praktik terbaik yang diakui secara internasional, tetapi juga membuktikan bahwa Tencent Cloud telah membangun sistem manajemen keamanan cloud yang lebih komprehensif, sehingga meningkatkan kemampuan layanan keamanan cloud secara keseluruhan.

Sertifikasi ISO/IEC 27018: 2014 ISO/IEC 27018: 2014 merupakan standar keamanan global yang paling komprehensif dan diakui untuk penanganan Informasi Pribadi Teridentifikasi (PII) dalam lingkungan cloud publik. Standar ini bertujuan menyediakan seperangkat pedoman praktis bagi penyedia layanan cloud guna melindungi privasi pengguna, serta memastikan keamanan data pribadi dalam lingkungan komputasi awan.

Perolehan sertifikasi ISO/IEC 27018: 2014 oleh Tencent Cloud menandakan bahwa sistem manajemen informasi pribadi Tencent Cloud mematuhi ketentuan hukum dan regulasi perlindungan informasi pribadi yang ketat secara internasional, sehingga memberikan kepercayaan dan jaminan lebih kepada pelanggan Tencent Cloud terkait keamanan cloud mereka.

Sertifikasi ISO/IEC 29151: 2017 ISO/IEC 29151: 2017 merupakan standar internasional yang digunakan untuk menerapkan langkah-langkah pengendalian terkait pemrosesan Informasi Pribadi Teridentifikasi (PII), guna memenuhi persyaratan yang ditentukan berdasarkan penilaian risiko dan dampak privasi yang terkait dengan perlindungan PII.

Tencent Cloud telah memperoleh sertifikasi ISO/IEC 29151: 2017. Hal ini menunjukkan bahwa Tencent Cloud telah mengembangkan sistem pengendalian keamanan yang sesuai berdasarkan tujuan PII dan kebutuhan bisnisnya, serta menyediakan kontrol perlindungan privasi tingkat tinggi untuk PII pengguna di lingkungan cloud.

Sertifikasi ISO/IEC 27701: 2019 merupakan persyaratan dan panduan perluasan dari ISO/IEC 27001 dan ISO/IEC 27002 dalam manajemen informasi privasi. Standar ini menyediakan pedoman untuk membangun, menerapkan, memelihara, dan terus meningkatkan Sistem Manajemen Informasi Privasi, yang menjadi tonggak penting dalam pengelolaan risiko privasi secara berkelanjutan.

Perolehan sertifikasi ISO/IEC 27701: 2019 oleh Tencent Cloud membuktikan bahwa Tencent Cloud senantiasa menempatkan perlindungan privasi pengguna sebagai inti layanannya. Hal ini secara penuh menggambarkan standarisasi dan keandalan perlindungan privasi dalam produk-produk Tencent Cloud.

2.3 Sertifikasi Regional & Industri

C5 Jerman Katalog Kriteria Kepatuhan Komputasi Awan (Cloud Computing Compliance Criteria Catalogue, disingkat C5) dikembangkan oleh Bundesamt für Sicherheit in der Informationstechnik (BSI) Jerman, dengan tujuan memverifikasi kepatuhan keamanan informasi penyedia layanan cloud melalui pemeriksaan dan pelaporan yang terstandarisasi. C5 adalah standar keamanan tingkat tinggi yang sangat diakui dalam industri layanan cloud.

Tencent Cloud telah lulus audit standar dasar dan tambahan C5:2020 Jerman. Hal ini menunjukkan bahwa Tencent Cloud telah memenuhi standar tinggi yang ditetapkan oleh pemerintah Jerman dalam hal perlindungan data dan keamanan informasi.

TISAX Jerman TISAX adalah standar penilaian keamanan informasi dan keamanan pertukaran data untuk industri otomotif yang diluncurkan oleh Asosiasi Industri Otomotif Jerman (VDA) bekerja sama dengan Asosiasi Pertukaran Data Keamanan Industri Otomotif Eropa (ENX). TISAX memungkinkan saling pengakuan

hasil penilaian keamanan informasi di dalam industri otomotif dan menyediakan mekanisme penilaian serta pertukaran yang seragam.

Saat ini, sejumlah Pusat Data Internet (IDC) milik Tencent Cloud (termasuk yang berlokasi di Beijing, Shenzhen, dan lainnya) telah lulus audit penilaian TISAX Tingkat 3. Hal ini menunjukkan bahwa layanan yang disebarkan di wilayah-wilayah tersebut memenuhi persyaratan TISAX dan telah membangun serta memelihara sistem manajemen keamanan informasi yang komprehensif.

Sertifikasi MTCS T3 Singapura Standar Keamanan Cloud Berlapis Singapura (MTCS) dirumuskan di bawah bimbingan Komite Standar Teknologi Informasi (ITSC) dari Otoritas Pengembangan Infokom Singapura (IMDA). Sebagai standar umum untuk cloud, penyedia layanan cloud dapat mengadopsi standar ini untuk mengatasi kekhawatiran pelanggan mengenai keamanan dan kerahasiaan data di cloud, serta dampak penggunaan layanan cloud terhadap bisnis.

Tencent Cloud telah berhasil memperoleh sertifikasi standar tingkat T3 dari MTCS (Multi-Tier Cloud Security) Singapura. Sertifikasi ini menunjukkan bahwa Tencent Cloud telah menerapkan mekanisme manajemen risiko yang kuat untuk menjamin keamanan, kerahasiaan, serta transparansi operasional yang dapat diverifikasi bagi data pelanggan di cloud.

OSPAR Singapura Laporan Audit Penyedia Layanan Outsourcing (Outsourced Service Provider Audit Report, OSPAR) adalah standar akses untuk layanan outsourcing di industri keuangan Singapura. Standar ini didasarkan pada SSAE 3000 Singapura, bertujuan memverifikasi desain kontrol dan efektivitas operasional terkait di tiga bidang bagi penyedia layanan institusi keuangan Singapura: kontrol tingkat entitas, kontrol teknologi informasi umum, dan kontrol layanan.

Berbagai produk dan layanan Tencent Cloud telah lulus audit OSPAR Singapura, dan Tencent Cloud secara konsisten berupaya memastikan bahwa kontrolnya mematuhi pedoman dari Asosiasi Perbankan Singapura (ABS). Keberhasilan dalam audit ini menunjukkan bahwa kemampuan keamanan Tencent Cloud

memenuhi persyaratan ketat industri jasa keuangan di Singapura bahkan Asia Tenggara.

Data Protection Trustmark Singapura	Data Protection Trustmark (DPTM) dikembangkan oleh Komisi Perlindungan Data Pribadi Singapura (PDPC) bersama Otoritas Pengembangan Infokom Media (IMDA), bertujuan menunjukkan praktik perlindungan data yang bertanggung jawab oleh organisasi.
-------------------------------------	--

Tencent Cloud telah memperoleh sertifikasi Data Protection Trustmark (DPTM) Singapura. Hal ini menunjukkan bahwa Tencent Cloud telah mengadopsi praktik perlindungan data yang bertanggung jawab bagi pelanggan, mitra bisnis, dan regulator, serta memiliki kemampuan untuk melindungi data pribadi yang dikumpulkannya.

Cyber Trust Mark (CTM) Singapura	Cyber Trust Mark (CTM) adalah sertifikasi keamanan siber tingkat nasional yang diluncurkan oleh Badan Keamanan Siber Singapura (Cyber Security Agency/CSA). Kerangka kerja CTM mengadopsi metodologi berbasis risiko, mencakup 22 subdomain dalam 4 area inti: tata kelola dan manajemen risiko, operasi keamanan siber, ketahanan, keamanan rantai pasok dan sumber daya manusia, serta peningkatan berkelanjutan dan praktik-praktik terdepan.
----------------------------------	--

Tencent Cloud telah meraih tingkat tertinggi (Tier 5) dari Cyber Trust Mark (CTM). Sertifikasi ini menegaskan kemampuan Tencent Cloud yang unggul dalam tata kelola keamanan siber, manajemen risiko, dan ketahanan operasional, sekaligus memposisikannya sebagai penyedia layanan cloud terpercaya bagi sektor-sektor yang diregulasi ketat dan berkebutuhan tinggi di seluruh kawasan Asia-Pasifik.

Sertifikasi KISMS Korea	Sertifikasi Sistem Manajemen Keamanan Informasi Korea (K-ISMS) adalah sertifikasi keamanan informasi yang didukung pemerintah Korea, bertujuan membantu perusahaan dan organisasi Korea secara konsisten melindungi aset informasi mereka dengan aman sesuai hukum teknologi informasi dan komunikasi Korea yang berlaku.
-------------------------	---

Perolehan sertifikasi KISMS oleh Tencent Cloud menunjukkan bahwa pelanggan cloud di Korea lebih mudah membuktikan

kepatuhan mereka terhadap persyaratan hukum lokal, sehingga melindungi aset informasi digital kritis. Hal ini juga mencerminkan peningkatan kemampuan langkah-langkah penanganan keamanan informasi dan prosedur respons ancaman Tencent Cloud, yang dapat lebih efektif mengurangi dampak kerentanan keamanan.

Audit Kepatuhan TI Industri Keuangan Malaysia Bank Negara Malaysia (BNM), Suruhanjaya Sekuriti Malaysia (SC), dan regulator keuangan Malaysia lainnya telah mengeluarkan peraturan terkait yang ditujukan bagi industri jasa keuangan, guna menstandardisasi penerapan teknologi informasi di perbankan, asuransi, sekuritas, dan layanan keuangan lainnya di Malaysia, serta menjamin keandalan, keamanan, dan stabilitas sistem informasi keuangan.

Melalui audit pihak ketiga independen, Tencent Cloud dapat membuktikan bahwa layanan cloud yang disediakan bagi klien keuangan di Malaysia mematuhi secara ketat persyaratan regulasi industri keuangan Malaysia.

Audit Kepatuhan TI Industri Keuangan Hong Kong Otoritas Moneter Hong Kong (HKMA), Komisi Sekuritas dan Berjangka (SFC), serta Otoritas Asuransi (IA) Hong Kong telah menerbitkan sejumlah persyaratan pengawasan kunci guna mengatur penerapan teknologi informasi di lembaga keuangan, asuransi, dan sekuritas.

Melalui audit pihak ketiga independen, Tencent Cloud membuktikan dirinya sebagai penyedia layanan cloud yang dapat dipercaya di industri keuangan. Tencent Cloud telah mengambil pendekatan proaktif untuk memenuhi kewajiban kepatuhan yang paling ketat, sehingga lembaga keuangan dapat dengan percaya membangun layanan keuangan generasi berikutnya di atas platform Tencent Cloud.

Audit Kepatuhan TI Industri Keuangan Thailand Audit Kepatuhan TI Industri Keuangan Thailand: Lembaga industri keuangan Thailand harus mematuhi peraturan terkait yang dikeluarkan oleh Bank Sentral Thailand (BoT), Kantor Komisi Sekuritas dan Bursa (OSEC), Kantor Komisi Asuransi (OIC), dan badan pengatur serta otoritas hukum terkait lainnya. Persyaratan pengawasan ini mencakup: manajemen risiko dalam penerapan

teknologi informasi, perlindungan informasi pribadi, serta penerapan dan kontrol keamanan teknologi informasi dalam sistem perbankan, asuransi, sistem pemerintahan elektronik, uang elektronik, infrastruktur sistem pembayaran, penyedia layanan pembayaran, dan lain-lain.

Melalui audit pihak ketiga independen, Tencent Cloud dapat membuktikan kemampuannya dalam mematuhi persyaratan pengawasan industri keuangan Thailand yang ketat, serta komitmen Tencent Cloud untuk menyediakan layanan cloud yang berkualitas dan sesuai dengan regulasi bagi klien industri keuangan Thailand.

Audit Kepatuhan TI Industri Keuangan Indonesia	Bank Indonesia (BI), Otoritas Jasa Keuangan (OJK), dan regulator keuangan Indonesia lainnya telah mengeluarkan peraturan terkait yang ditujukan bagi industri jasa keuangan. Persyaratan pengawasan ini mencakup: manajemen risiko dalam penerapan teknologi informasi, perlindungan informasi pribadi, serta penerapan dan kontrol keamanan teknologi informasi dalam sistem perbankan, asuransi, sistem pemerintahan elektronik, uang elektronik, infrastruktur sistem pembayaran, penyedia layanan pembayaran, dan lain-lain.
--	--

Tencent Cloud telah lulus audit kepatuhan keuangan Indonesia yang dilaksanakan oleh lembaga audit pihak ketiga independen. Hal ini membuktikan bahwa layanan cloud yang disediakan Tencent Cloud bagi klien keuangan di Indonesia mematuhi secara ketat persyaratan regulasi industri keuangan Indonesia.

Sertifikasi Manajemen Keamanan Informasi SNI 27001 Indonesia	SNI 27001 Indonesia adalah standar nasional untuk Sistem Manajemen Keamanan Informasi (ISMS) yang diawasi oleh Badan Standardisasi Nasional (BSN) dan disertifikasi oleh lembaga audit pihak ketiga independen. Kerangka SNI 27001 mengadopsi pendekatan berbasis risiko, dengan persyaratan inti yang mencakup dimensi kunci: pembentukan dan operasi berkelanjutan ISMS formal, penilaian risiko komprehensif dan langkah pengendalian yang ditargetkan, kepatuhan terhadap regulasi keamanan informasi lokal serta 14 bidang keamanan utama, serta audit internal, tinjauan manajemen, dan peningkatan berkelanjutan secara berkala.
---	---

Perolehan sertifikasi SNI 27001 Indonesia oleh Tencent Cloud membuktikan kemampuan unggul Tencent Cloud dalam melindungi kerahasiaan, integritas, dan ketersediaan aset informasi, yang juga mencakup skenario keamanan khusus di lingkungan cloud. Hal ini mencerminkan sistem manajemen keamanan Tencent Cloud yang matang serta kemampuannya dalam menghadapi risiko siber yang terus berkembang di pasar Indonesia.

Audit Kepatuhan TI Industri Keuangan Filipina Lembaga industri keuangan Filipina harus mematuhi peraturan terkait yang ditetapkan oleh Bank Sentral Filipina (BSP) dan badan pengatur serta otoritas hukum terkait lainnya dalam sektor keuangan. Persyaratan pengawasan ini mencakup: manajemen risiko dalam penerapan teknologi informasi, perlindungan informasi pribadi, serta penerapan dan kontrol keamanan teknologi informasi dalam sistem perbankan, asuransi, sistem pemerintahan elektronik, uang elektronik, infrastruktur sistem pembayaran, penyedia layanan pembayaran, dan lainnya.

Melalui audit pihak ketiga independen, Tencent Cloud dapat membuktikan kemampuannya dalam mematuhi persyaratan pengawasan industri keuangan Filipina yang ketat, serta komitmennya untuk menyediakan layanan cloud yang berkualitas dan sesuai regulasi bagi klien industri keuangan.

Asosiasi Gambar Bergerak Amerika (MPAA) Asosiasi Gambar Bergerak Amerika (MPAA) telah menetapkan seperangkat standar praktik terbaik untuk penyimpanan, pemrosesan, dan transmisi konten media yang dilindungi yang aman. Panduan implementasi ini bertujuan untuk memberi pemahaman kepada penyedia aplikasi dan layanan cloud yang bermitra dengan anggota MPAA mengenai persyaratan yang harus dipatuhi dalam hal keamanan konten. Komponen templat keamanan konten MPAA mengacu pada standar ISO terkait (27001-27002), standar keamanan (seperti NIST, CSA, ISACA, dan SANS), serta praktik terbaik industri.

Tencent Cloud telah memperoleh sertifikasi terkait seperti ISO 27001, ISO 27017, ISO 27018, PCI DSS, dan CSA STAR. Selain itu, melalui penilaian mandiri, Tencent Cloud memastikan bahwa prosedur pengelolaan konten pelanggannya mematuhi panduan

model keamanan konten Asosiasi Gambar Bergerak Amerika (MPAA).

HIPAA Amerika Serikat Salah satu tujuan dari Undang-Undang HIPAA Amerika Serikat adalah mendorong penggunaan rekam medis elektronik dengan meningkatkan efisiensi dan kualitas sistem perawatan kesehatan melalui peningkatan berbagi informasi. HIPAA berfokus dan menjamin keamanan (termasuk ketersediaan, integritas, dan kerahasiaan) serta privasi dari Informasi Kesehatan yang Dilindungi (Protected Health Information, PHI) dalam siklus pembuatan, penerimaan, pemeliharaan, dan transmisi oleh entitas yang tercakup serta mitra bisnisnya. Entitas yang tunduk pada HIPAA dan mitra bisnis mereka diharuskan menerapkan langkah-langkah keamanan yang sesuai dalam skenario pemrosesan, pemeliharaan, dan penyimpanan PHI.

Tencent Cloud, melalui penilaian mandiri, memastikan bahwa kemampuan perlindungan keamanan informasi pribadi pengguna dan efektivitas langkah-langkah kontrolnya mematuhi persyaratan kepatuhan HIPAA.

Aturan SEC 17a-4 Amerika Serikat Layanan Penyimpanan Objek Tencent Cloud (COS) telah disertifikasi oleh perusahaan penilaian pihak ketiga independen yang berspesialisasi dalam manajemen catatan dan tata kelola informasi, sesuai dengan persyaratan teknis dari Komisi Sekuritas dan Bursa AS (SEC), Otoritas Regulasi Industri Keuangan (FINRA), dan Komisi Perdagangan Berjangka Komoditas (CFTC).

Sertifikasi ini menjamin bagi pelanggan yang beroperasi di lingkungan yang sangat diatur (seperti industri jasa keuangan) mengenai metode penyimpanan yang tidak dapat ditimpa dan tidak dapat dihapus serta kemampuan penguncian objek dari Tencent COS, menunjukkan komitmen Tencent Cloud untuk menyediakan produk cloud yang aman dan sesuai dengan standar industri bagi pelanggan.

FISC Jepang Untuk meningkatkan keamanan lembaga keuangan, Panduan Keamanan Sistem Komputer Bank dan Lembaga Keuangan Terkait (FISC) memberikan arahan efektif bagi bank dan lembaga

keuangan Jepang dalam membangun sistem informasi yang aman serta menjamin pengoperasian sistem informasi.

Berdasarkan panduan ini, Tencent Cloud telah melakukan penilaian terhadap status kontrol saat ini untuk memastikan bahwa langkah-langkah terkait yang diterapkan Tencent Cloud memenuhi persyaratan yang ditetapkan dalam Panduan Keamanan Sistem Komputer Bank dan Lembaga Keuangan Terkait (FISC).

BS 10012: 2017 Inggris
BS 10012: 2017 diterbitkan oleh British Standards Institution (BSI) yang bertujuan menyediakan kerangka kepatuhan dan praktik terbaik perlindungan privasi bagi organisasi, serta membimbing perusahaan dalam membangun dan memelihara Sistem Manajemen Informasi Pribadi (PIMS) guna memastikan organisasi memiliki langkah-langkah pengendalian yang memadai dan tepat untuk melindungi informasi pribadi. Sistem ini telah diperbarui dan direvisi agar sesuai dengan General Data Protection Regulation (GDPR).

Tencent Cloud telah memperoleh sertifikasi BS 10012: 2017, yang mencerminkan bahwa Sistem Manajemen Informasi Pribadi Tencent Cloud memenuhi persyaratan standar internasional dan praktik terbaik industri, sehingga memungkinkan pelanggan untuk lebih patuh terhadap persyaratan perlindungan privasi GDPR.

CISPE Uni Eropa
Kode Etik CISPE (Cloud Infrastructure Services Providers in Europe) adalah pedoman sektoral pan-Eropa khusus untuk penyedia layanan infrastruktur cloud berdasarkan Pasal 40 Peraturan Perlindungan Data Umum (GDPR) Uni Eropa. Kode etik ini membantu organisasi di seluruh Eropa mempercepat pengembangan layanan berbasis cloud yang sesuai dengan GDPR bagi konsumen, bisnis, dan institusi.

Tencent Cloud telah diberikan label "Kandidat" untuk Kode Etik CISPE. Hal ini menunjukkan bahwa Tencent Cloud telah menyelesaikan penilaian mandiri sesuai dengan persyaratan Kode Etik CISPE, yang digunakan untuk membuktikan kepatuhan Tencent Cloud pada tingkat dokumentasi dan implementasi.

Sertifikasi NIST CSF	Kerangka Kerja Siber NIST (NIST CSF) adalah sebuah kerangka kerja yang berfokus pada penggunaan pendorong bisnis untuk mengarahkan aktivitas keamanan siber, memperlakukan risiko keamanan siber sebagai bagian dari proses manajemen risiko organisasi, serta membantu organisasi menyesuaikan dan memprioritaskan kegiatan keamanan siber mereka berdasarkan kebutuhan bisnis, toleransi risiko, dan sumber daya yang dimiliki. Organisasi dapat meningkatkan keamanan dan ketahanan mereka dengan menerapkan prinsip dan panduan manajemen risiko dari kerangka kerja ini.
-------------------------	---

Tencent Cloud telah memperoleh sertifikasi NIST CSF yang diverifikasi oleh lembaga pihak ketiga. Hal ini tidak hanya merupakan pengakuan atas kemampuan sistem pertahanan keamanan siber Tencent Cloud, tetapi juga menunjukkan bahwa Tencent Cloud mampu secara efektif mengidentifikasi, menahan, merespons, dan menangani risiko keamanan, serta melindungi aset cloud dan data pelanggan. Hal ini selanjutnya meningkatkan kepercayaan pelanggan terhadap stabilitas dan keamanan Tencent Cloud.

Sertifikasi PCI DSS	Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) dibuat dan dikelola oleh Dewan Standar Keamanan Industri Kartu Pembayaran (PCI SSC). Untuk meningkatkan keamanan data pemegang kartu, PCI DSS menyediakan tolok ukur global yang seragam untuk persyaratan teknis dan operasional dalam melindungi data akun, dengan ruang lingkup yang mencakup semua entitas yang terlibat dalam pemrosesan kartu pembayaran, seperti pedagang, pengolah, akuisitor, penerbit, dan penyedia layanan, serta entitas lain yang menyimpan, memproses, atau mengirimkan data pemegang kartu.
------------------------	--

Tencent Cloud telah lulus audit sertifikasi PCI DSS dan memperoleh kualifikasi Penyedia Layanan PCI DSS Level 1. Hal ini membuktikan bahwa Tencent Cloud dapat menyediakan layanan pembayaran yang aman dan andal bagi pelanggan serta melindungi keamanan data pemegang kartu.

Kepatuhan GxP	Dalam industri perawatan kesehatan, GxP mencakup beragam aktivitas terkait kepatuhan yang luas. Secara umum, GxP mengacu pada seperangkat peraturan, pedoman, atau praktik terbaik industri yang mengatur pengembangan, manufaktur, dan penjualan produk perawatan kesehatan seperti obat-obatan, perangkat medis, dan aplikasi perangkat lunak medis. Tencent Cloud telah menerbitkan Buku Putih Kepatuhan GxP, yang menjelaskan kepada pelanggan di industri perawatan kesehatan bahwa proses manajemen dan langkah-langkah teknis Tencent Cloud dapat membantu mereka memenuhi persyaratan sistem terkomputerisasi GxP. Selain itu, hal ini memastikan kerahasiaan, integritas, dan ketersediaan data bisnis pelanggan yang dihosting di Tencent Cloud.
---------------	--

03

Model Tanggung Jawab Bersama untuk Keamanan Cloud Tencent

Saat ini, semakin banyak pelanggan yang menjadikan keamanan sebagai salah satu faktor pertimbangan utama dalam memilih penyedia layanan komputasi awan beserta produk dan layanan yang ditawarkannya. Tencent Cloud berpegang pada karakteristik terbuka dan berbagi dari layanan komputasi awan, terus meningkatkan kemampuan keamanan platform dan layanan cloud, serta bersama-sama dengan pelanggan membangun sistem perlindungan keamanan yang lebih baik dan lebih lengkap untuk bisnis dan data di cloud. Sebagai penyedia layanan cloud, Tencent Cloud bertanggung jawab atas infrastruktur pusat data dan keamanan platform cloud. Mengingat bahwa ketika pelanggan memilih kategori layanan cloud yang berbeda (seperti layanan IaaS, PaaS, dan SaaS), tingkat kendali atas komponen yang berbeda juga akan bervariasi. Untuk itu, Tencent Cloud telah membangun model Tanggung Jawab Bersama untuk Keamanan Cloud berdasarkan berbagai kategori layanan cloud. Dalam model ini, area berwarna biru muda menjadi tanggung jawab Tencent Cloud, area berwarna abu-abu muda menjadi tanggung jawab pelanggan, sedangkan area berwarna hijau muda menunjukkan tanggung jawab bersama yang akan dipikul oleh Tencent Cloud dan pelanggan.

	IaaS	PaaS	SaaS	
Tanggung Jawab Klien	Keamanan Data Pelanggan Cloud	Keamanan Data Pelanggan Cloud	Keamanan Data Pelanggan Cloud	Tanggung Jawab Bersama untuk Layanan/Skenario Berbeda
	Kebijakan Akun dan Kontrol Akses Pelanggan Cloud	Kebijakan Akun dan Kontrol Akses Pelanggan Cloud	Kebijakan Akun dan Kontrol Akses Pelanggan Cloud	
	Kebijakan Konfigurasi Keamanan di Cloud	Kebijakan Konfigurasi Keamanan di Cloud	Kebijakan Konfigurasi Keamanan di Cloud	
	Keamanan Aplikasi di Cloud	Keamanan Aplikasi di Cloud	Keamanan Aplikasi di Cloud	
	Keamanan Jaringan Virtual dan Host di Cloud	Keamanan Jaringan Virtual dan Host di Cloud	Keamanan Jaringan Virtual dan Host di Cloud	
	Kepatuhan dan Keamanan Platform Cloud serta Produk Cloud itu Sendiri	Kepatuhan dan Keamanan Platform Cloud serta Produk Cloud itu Sendiri	Kepatuhan dan Keamanan Platform Cloud serta Produk Cloud itu Sendiri	Tanggung Jawab Bersama Tencent Cloud
	Keamanan Fisik dan Infrastruktur	Keamanan Fisik dan Infrastruktur	Keamanan Fisik dan Infrastruktur	

Gambar 1: Model Tanggung Jawab Bersama Keamanan Informasi Tencent Cloud

Penjelasan Tencent Cloud terhadap atribut keamanan yang berbeda dalam gambar di atas adalah sebagai berikut:

- **Keamanan Data Pelanggan Cloud:** Mengacu pada manajemen keamanan data bisnis pelanggan itu sendiri di lingkungan komputasi awan, termasuk data bisnis pelanggan yang diunggah, disimpan, didistribusikan, diproses, atau ditangani dengan cara lain.
- **Kebijakan Akun dan Kontrol Akses Pelanggan Cloud:** Mengacu pada informasi akun Tencent Cloud yang didaftarkan oleh pelanggan, serta semua tindakan otorisasi di bawah akun cloud, termasuk informasi akun, kata sandi, kebijakan kontrol akses, autentikasi, dan sebagainya.
- **Kebijakan Konfigurasi Keamanan di Cloud:** Mengacu pada produk keamanan dan kebijakan konfigurasi keamanan yang sesuai dengan persyaratan keamanan bisnis yang berbeda berdasarkan skenario tertentu, untuk mengembangkan atau menggunakan produk cloud (termasuk produk keamanan) dengan benar.
- **Keamanan Aplikasi di Cloud:** Mengacu pada manajemen keamanan sistem aplikasi terkait bisnis di lingkungan komputasi awan, termasuk desain, pengembangan, rilis, operasi, pemeliharaan, dan pemantauan aplikasi.
- **Keamanan Jaringan Virtual dan Host di Cloud:** Mengacu pada manajemen keamanan host dan jaringan di lingkungan komputasi awan. Pada tingkat jaringan, mencakup jaringan virtual, penyeimbangan beban, gateway keamanan, VPN, sambungan khusus, dan sebagainya; pada tingkat host, mencakup manajemen dasar (seperti lapisan kontrol virtualisasi, sistem manajemen basis data, jaringan disk array, dll.) dan manajemen penggunaan (seperti host virtual, citra, CDN, sistem file, dll.) untuk produk cloud seperti komputasi awan, penyimpanan awan, dan basis data awan.

- **Kepatuhan dan Keamanan Platform Cloud serta Produk Cloud itu Sendiri:** Mengacu pada keamanan dan kepatuhan platform cloud serta produk/layanan cloud yang disediakan di lingkungan komputasi awan.
- **Keamanan Fisik dan Infrastruktur:** Mengacu pada operasi keamanan pusat data, serta manajemen keamanan server fisik dan perangkat jaringan fisik di lingkungan komputasi awan.

Untuk informasi lebih lanjut tentang Model Tanggung Jawab Bersama Keamanan, silakan lihat [Tencent Cloud Security White Paper](#).

04

Infrastruktur Global Tencent Cloud

Tencent Cloud telah menyebarkan banyak pusat data di seluruh dunia, membentuk jaringan infrastruktur yang luas yang mampu menyediakan layanan cepat, stabil, cerdas, dan andal di lokasi terdekat bagi pelanggan global. Tencent Cloud telah membuka 20+ wilayah geografis (Region) dan mengoperasikan 60+ zona ketersediaan (Availability Zone) di Tiongkok Daratan, kawasan Asia Pasifik, Amerika Utara, dan Eropa. Ini memberikan dukungan teknis yang kuat untuk lebih banyak perusahaan, membantu ekspansi bisnis yang pesat, memungkinkan pelanggan merespons persyaratan peraturan di berbagai wilayah secara fleksibel, memenuhi kebutuhan perusahaan industri keuangan akan penyimpanan data lokal dan globalisasi bisnis, serta memastikan kepatuhan, keamanan, dan efisiensi dalam pemrosesan data.

- Wilayah (Region) mengacu pada area geografis fisik tempat pusat data berada. Wilayah-wilayah Tencent Cloud sepenuhnya terisolasi satu sama lain, memastikan stabilitas dan toleransi kesalahan maksimum antarwilayah. Untuk mengurangi latensi akses dan meningkatkan kecepatan unduh, disarankan agar pelanggan memilih wilayah yang terdekat.
- Zona Ketersediaan (Zone) adalah pusat data fisik di dalam wilayah yang sama dengan pasokan listrik dan jaringan yang saling independen. Tujuannya adalah memastikan bahwa kegagalan di satu zona ketersediaan tidak menyebar ke zona lain (kecuali dalam kasus bencana besar atau gangguan listrik skala besar), sehingga layanan bisnis pengguna tetap berjalan. Dengan meluncurkan instans di zona ketersediaan yang terpisah, pengguna dapat melindungi aplikasi mereka dari dampak kegagalan di satu lokasi.

Tencent Cloud saat ini telah menerapkan 2.300+ node akselerasi di dalam Tiongkok, mencakup berbagai operator. Di luar Tiongkok, terdapat 900+ node akselerasi yang mencakup 70+ negara dan wilayah di seluruh dunia. Dengan mendistribusikan konten layanan ke seluruh node akselerasi di jaringan dan menggunakan sistem penjadwalan global, pengguna dapat mengakses konten

yang diperlukan dari node terdekat, sehingga mengurangi latensi akses.

Tencent Cloud juga meningkatkan isolasi dan keamanan data dengan membangun situs independen serta menerapkan teknologi seperti enkripsi data, kontrol akses, dan pelacakan audit, mencegah kebocoran data dan akses tidak sah, serta memperkuat isolasi data berdasarkan wilayah dan penanganan yang sesuai dengan regulasi.

Untuk informasi lebih lanjut tentang infrastruktur Tencent Cloud, silakan kunjungi halaman [Tencent Cloud Global Infrastructure](#).

05

Bagaimana Tencent Cloud Membantu Mematuhi dan Mendukung Pelanggan Dalam Memenuhi Persyaratan Manajemen Risiko Terkait Penggunaan Teknologi Informasi Perbankan Komersial

Inovasi berkelanjutan dalam teknologi informasi memberikan dukungan kunci bagi pemberdayaan bisnis perbankan. Dengan menerapkan teknologi informasi secara efektif, bank umum dapat secara signifikan meningkatkan efisiensi operasi internal dan mengoptimalkan kualitas layanan kepada pelanggan. Namun, penerapan teknologi informasi yang mendalam dalam aktivitas operasional bank juga meningkatkan risiko yang dihadapi oleh bank. Penggunaan teknologi informasi perlu memperhatikan dinamika perubahan aturan regulasi yang relevan serta perkembangan standar nasional dan internasional. Pada tahun 2016, Otoritas Jasa Keuangan Indonesia menerbitkan [NOMOR 38 /POJK.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum](#) guna mengatur dan menyempurnakan manajemen risiko dalam proses penggunaan teknologi informasi oleh bank umum. Klausul-klausulnya terutama berkisar pada penerapan manajemen risiko teknologi informasi, operasi teknologi informasi oleh bank dan/atau penyedia layanan teknologi informasi, layanan perbankan elektronik, pelaporan, dan aspek lainnya. Pada tahun 2020, Otoritas Jasa Keuangan merevisi persyaratan regulasi ini dengan menerbitkan [NOMOR 13 /POJK.03/2020 Tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan NOMOR 38/POJK.03/2016](#), yang merevisi persyaratan terkait pusat data dan pusat pemulihan bencana.

Untuk memberikan panduan lebih lanjut bagi bank umum dalam menerapkan manajemen risiko teknologi informasi, Otoritas Jasa Keuangan menerbitkan [NOMOR 21 /SEOJK.03/2017 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum](#) pada tahun 2017. Surat edaran ini menetapkan ketentuan pelaksanaan yang sesuai untuk berbagai persyaratan pengawasan dalam NOMOR 38 /POJK.03/2016, mencakup aspek-aspek seperti manajemen, pengembangan dan pengadaan, aktivitas operasional teknologi informasi, jaringan komunikasi, keamanan informasi, rencana pemulihan bencana, penggunaan penyedia layanan teknologi informasi, dan lainnya.

Dalam bab ini, Tencent Cloud akan merangkum dan menyimpulkan persyaratan kontrol yang terkait dengan penyedia layanan cloud dari NOMOR 38 /POJK.03/2016 beserta perubahannya, serta NOMOR 21 /SEOJK.03/2017. Selain itu, akan dijelaskan bagaimana Tencent Cloud, sebagai penyedia layanan cloud, dapat membantu bank umum mematuhi persyaratan terkait.

5.1 Manajemen Teknologi Informasi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
8	1.7	Kecukupan Kebijakan, Standar, dan Prosedur Penggunaan Teknologi Informasi di Bank	(1) Bank wajib memiliki kebijakan, standar, dan prosedur penggunaan Teknologi Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dan wajib menerapkan kebijakan, standar, dan prosedur penggunaan Teknologi Informasi secara konsisten dan berkesinambungan. (2) Kebijakan, standar, dan prosedur penggunaan Teknologi Informasi paling sedikit meliputi aspek: a. manajemen; b. pengembangan dan pengadaan; c. Operasional	Pelanggan harus menyusun kebijakan, standar, dan prosedur penggunaan teknologi informasi, serta melakukan tinjauan dan pembaruan secara berkala terhadap kebijakan dan prosedur tersebut, dan harus menetapkan toleransi tingkat risiko untuk memastikan aspek-aspek terkait teknologi informasi dapat beroperasi secara optimal. Guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar,

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		Teknologi Informasi; d. jaringan komunikasi; e. pengamanan informasi; f. Rencana Pemulihan Bencana; g. Layanan Perbankan Elektronik; h. penggunaan pihak penyedia jasa Teknologi Informasi; dan i. penyediaan jasa Teknologi Informasi oleh Bank. (3) Bank wajib menetapkan limit risiko yang dapat ditoleransi untuk memastikan aspek terkait Teknologi Informasi sebagaimana dimaksud pada ayat (2) dapat berjalan dengan optimal. (4) Bank wajib melakukan kaji ulang dan pengkinian kebijakan, standar dan prosedur sebagaimana dimaksud pada ayat (2) secara berkala.	prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Tim keamanan Tencent Cloud secara berkelanjutan memantau dan mengevaluasi risiko keamanan internal untuk menjaga efektivitas dan keandalan sistem manajemen keamanan informasi. Tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun, dan secara terus-menerus memantau kondisi platform cloud dan sistem internal, memastikan bahwa mereka mempertahankan postur keamanan yang baik dan mematuhi peraturan dan persyaratan standar manajemen keamanan serta peraturan perundang-undangan yang berlaku.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		(5) Bank wajib menetapkan jangka waktu kaji ulang dan pengkinian kebijakan, standar, dan prosedur sebagaimana dimaksud pada ayat (4) dalam kebijakan secara tertulis.	
10	1.8	Proses Manajeme n Risiko Terkait Teknologi Informasi	(1) Bank wajib memiliki kebijakan, standar, dan prosedur atas proses manajemen risiko Teknologi Informasi.	Pelanggan harus menetapkan dan menerapkan kebijakan, standar, serta prosedur terkait manajemen risiko teknologi informasi. Pelanggan perlu secara berkala melakukan penilaian risiko teknologi informasi, mengumpulkan aktivitas teknologi informasi yang berpotensi menimbulkan atau meningkatkan risiko, menganalisis secara kualitatif dan kuantitatif risiko yang telah diidentifikasi berdasarkan tingkat dampak dan frekuensi kemunculannya, menetapkan prioritas tindakan pengendalian, serta menerapkan langkah-langkah mitigasi risiko. Selain itu, pelanggan harus terus memantau dan melacak pelaksanaan kegiatan pengendalian dan mitigasi risiko yang telah diidentifikasi. Apabila pelanggan melibatkan penggunaan penyedia layanan teknologi informasi, maka pelanggan harus memastikan bahwa penyedia layanan tersebut juga menerapkan proses manajemen risiko yang sesuai.
			(2) Bank wajib melakukan proses manajemen risiko terkait penggunaan Teknologi Informasi.	
			(3) Proses manajemen risiko sebagaimana dimaksud pada ayat (2) dilakukan paling sedikit terhadap aspek terkait Teknologi Informasi sebagaimana dimaksud dalam Pasal 8 ayat (2).	
			(4) Dalam hal Bank menggunakan pihak penyedia jasa Teknologi Informasi, Bank wajib memastikan pihak penyedia jasa	
				Dalam rangka mendukung kepatuhan pelanggan terhadap

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		Teknologi Informasi menerapkan manajemen risiko sebagaimana diatur dalam Peraturan Otoritas Jasa Keuangan ini.	persyaratan regulasi, Tencent Cloud secara internal menetapkan prosedur manajemen risiko keamanan informasi, yang secara jelas mendefinisikan dan memberikan panduan untuk seluruh proses manajemen risiko (identifikasi risiko, analisis risiko, penyusunan rencana penanganan risiko, serta pelacakan dan pemantauan risiko). • Identifikasi Risiko: Tencent Cloud secara berkala melaksanakan penilaian risiko, mengidentifikasi skenario risiko yang relevan berdasarkan laporan insiden keamanan industri, pengalaman praktis Tencent Cloud, serta basis data risiko dari lembaga profesional. Identifikasi risiko dilakukan melalui analisis terhadap skenario risiko serta hasil analisis proses bisnis, produk, atau layanan. • Penilaian Risiko: Tencent Cloud mengevaluasi nilai aset, kemungkinan terjadinya risiko dalam skenario tertentu, serta tingkat dampak risiko, kemudian menghitung tingkat risiko berdasarkan parameter tersebut. • Penanganan Risiko: Berdasarkan hasil analisis risiko, Tencent Cloud menerapkan strategi respons dan langkah-langkah mitigasi yang sesuai untuk setiap risiko yang teridentifikasi. Untuk risiko tinggi,

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				penanggung jawab risiko menyusun rencana penanganan (melalui transfer risiko atau tindakan pengurangan risiko) dan memperbarui tabel manajemen risiko. Untuk risiko sedang, penanggung jawab risiko menilai kebutuhan penyusunan rencana penanganan berdasarkan kondisi aktual. Untuk risiko rendah, risiko tersebut dianggap dapat diterima. Tencent Cloud juga secara berkala meninjau risiko residual untuk memantau status dan nilai risikonya. • Pemantauan, Tinjauan, dan Pelaporan Risiko: Tencent Cloud mengumpulkan hasil penilaian risiko, menghasilkan laporan penilaian risiko, dan menyampaikannya kepada manajemen. Selain itu, Tencent Cloud memelihara tabel manajemen risiko, memantau perubahan kondisi risiko serta status rencana penanganan risiko, dan menyesuaikan rencana manajemen risiko secara real time. Selain itu, Tencent Cloud mendefinisikan indikator risiko kunci dan secara berkala melakukan pengukuran terhadap indikator tersebut. Dengan membandingkannya terhadap kriteria risiko yang dapat diterima, Tencent Cloud menganalisis akar penyebab masalah yang ditemukan serta mengusulkan rekomendasi dan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
solusi perbaikan.				

5.2 Langkah Pengendalian dalam Pengembangan dan Pengadaan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
11	2.2-2.3	Kebijakan, Standar, dan Prosedur Pengembangan dan Pengadaan	Dalam melakukan pengembangan dan pengadaan Teknologi Informasi, Bank wajib melakukan langkah pengendalian untuk menghasilkan sistem dan data yang terjaga kerahasiaan dan integrasi serta mendukung pencapaian tujuan Bank, antara lain mencakup: a. menetapkan dan menerapkan prosedur dan metodologi pengembangan dan pengadaan Teknologi Informasi secara konsisten; b. menerapkan manajemen proyek dalam pengembangan sistem;	Dalam melaksanakan pengembangan dan pengadaan teknologi informasi, pelanggan harus menetapkan dan menjalankan prosedur serta rencana pengembangan dan pengadaan teknologi informasi, menerapkan manajemen proyek, melakukan pengujian yang memadai, serta mendokumentasikan seluruh proses. Selain itu, pelanggan perlu membangun mekanisme manajemen perubahan sistem aplikasi untuk memastikan kemampuan pelacakan lengkap (full traceability) pada sistem teknologi informasi. Apabila perangkat lunak yang digunakan pelanggan dikembangkan oleh pihak ketiga dan tidak menyediakan kode sumber (source code), pelanggan perlu mengevaluasi kebutuhan untuk menandatangani perjanjian escrow tertulis dengan pihak ketiga tersebut. Untuk mendukung pelanggan dalam manajemen pengembangan, Tencent Cloud menyediakan alat pengembang Cloud Native Build

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			c. melakukan uji coba yang memadai pada saat pengembangan dan pengadaan suatu sistem, termasuk uji coba bersama satuan kerja pengguna, untuk memastikan keakuratan dan berfungsinya sistem sesuai kebutuhan pengguna serta kesesuaian sistem yang satu dengan sistem yang lain;	(CNB). CNB berbasis ekosistem Docker, yang mengabstraksikan lingkungan, cache, dan plugin, serta menggunakan sintaks deklaratif, bertujuan membantu pengembang membangun perangkat lunak dengan cara yang lebih efisien. CNB menyediakan rangkaian lengkap alat pengembang, dengan kemampuan seperti hosting kode, pipeline pengembangan berkinerja tinggi, peninjauan kode AI, lingkungan pengembangan berbasis cloud, manajemen artefak, dan kumpulan tugas yang dapat disesuaikan, yang secara efektif dapat mendukung seluruh alur proses pengembangan dari kebutuhan hingga penyebaran serta manajemen pengembangan yang gesit. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN, General Service Level Agreement, Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan
			d. melakukan dokumentasi atas pengembangan dan pemeliharaan sistem;	
			e. memiliki manajemen perubahan sistem aplikasi;	
			f. memastikan sistem Teknologi Informasi Bank mampu menampilkan kembali informasi secara utuh; dan	
			g. mengukur urgensi pembuatan perjanjian tertulis (escrow agreement) atas perangkat lunak yang dianggap penting untuk kelangsungan	

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		operasional Bank dalam hal perangkat lunak dibuat oleh pihak lain dan kode sumber tidak diberikan kepada Bank.	dalam perjanjian tersebut. Untuk mendukung pelanggan dalam memenuhi persyaratan regulasi, dalam hal pengembangan keamanan sistem, Tencent Cloud telah membangun seperangkat standar pengembangan keamanan sistem informasi internal. Tencent Cloud berupaya mengintegrasikan standar ISO/IEC 20000 Manajemen Layanan Teknologi Informasi, ISO/IEC 27001 Sistem Manajemen Keamanan Informasi, dan ISO/IEC 9001 Sistem Manajemen Mutu ke dalam seluruh siklus hidup pengembangan keamanan produk. Hal ini dilakukan dengan memperhatikan berbagai tahapan seperti analisis kebutuhan, desain, pengembangan, pengujian, penerapan, dan pemeliharaan, untuk menghilangkan masalah keamanan informasi dan privasi pada setiap tahap pengembangan produk, serta memastikan bahwa produk cloud mendapatkan pengendalian keamanan yang memadai selama siklus hidupnya. Tindakan pengendalian keamanan terkait meliputi: • Pelatihan Keamanan: Meningkatkan kesadaran pemrograman aman di kalangan pengembang, dan secara ketat mewajibkan personel terkait untuk mematuhi standar pengkodean yang aman. • Analisis Kebutuhan:

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			Berkomunikasi mengenai konten bisnis, alur proses bisnis, dan kerangka teknologi untuk menemukan cara optimal dalam mengintegrasikan keamanan. - Desain Sistem: Melakukan pemodelan ancaman terhadap desain sistem, serta menilai keamanan teknologi dari arsitektur yang digunakan. - Pengembangan Sistem: Selama proses pengembangan, menyediakan komponen pengembangan aman yang dirancang sendiri oleh Tencent untuk digunakan oleh tim pengembang, dan melakukan pengkodean sesuai dengan standar pengkodean aman Tencent Cloud. - Verifikasi Keamanan: Mendeteksi kerentanan melalui pemeriksaan keamanan kode, pemindaian keamanan aset, pemindaian web, penilaian keamanan manual, pengujian penetrasi, dan audit kode. - Rilis: Sistem hanya dapat dirilis ke lingkungan produksi setelah semua risiko tinggi diperbaiki, guna mencegah produk dijalankan di lingkungan produksi dengan membawa kerentanan keamanan. Dalam hal pengujian sistem, setelah tim pengembangan Tencent Cloud menyelesaikan pengembangan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				produk baru atau ketika produk mengalami perubahan signifikan, personel penguji menyusun rencana pengujian dan kasus uji yang sesuai berdasarkan kebutuhan produk, serta mengorganisir tim proyek untuk meninjau kasus uji tersebut. Setelah kasus uji dikonfirmasi, tim pengujian melakukan pengujian fungsional pada produk proyek untuk memastikan fungsionalitas produk tersedia, andal, dan memenuhi persyaratan kualitas produk yang ditetapkan secara internal oleh Tencent Cloud. Setelah pengujian fungsional selesai, tim keamanan melakukan pengujian keamanan pada produk. Cacat atau kerentanan yang ditemukan selama proses pengujian ditangani sesuai dengan alur manajemen kerentanan internal Tencent Cloud. Personel penguji menghasilkan laporan pengujian berdasarkan hasil pengujian dan menyerahkannya kepada berbagai tim terkait untuk konfirmasi. Terhadap penggunaan produk pihak ketiga, Tencent Cloud menetapkan persyaratan manajemen keamanan rantai pasok perangkat lunak, dengan jelas menetapkan tinjauan keamanan saat masuknya komponen eksternal, serta melakukan penguatan dan pertahanan keamanan sebelum peluncuran, untuk memastikan produk lulus pemeriksaan keamanan pra-peluncuran. Setelah diluncurkan, produk akan menjalani operasi dan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			pemeriksaan keamanan berkelanjutan, menangani masalah keamanan secara tepat waktu, serta melalui evaluasi kondisi operasi keamanan produk untuk mengidentifikasi risiko keamanan, mendorong pemasok untuk melakukan perbaikan, dan meninjau strategi kerja sama selanjutnya dengan pemasok tersebut. Dalam hal manajemen perubahan, Tencent Cloud telah menetapkan seperangkat standar manajemen untuk perubahan produk dan konfigurasi. Semua jenis perubahan program, termasuk perubahan pada aplikasi dan file konfigurasi, sistem operasi, serta basis data, harus melalui analisis dampak bisnis sebelum diluncurkan, menyusun rencana rollback untuk perubahan tersebut, dan mendapatkan persetujuan dari penanggung jawab terkait. Sistem rilis perubahan Tencent Cloud mewajibkan bahwa operasi perubahan hanya dapat dilakukan oleh personel yang berwenang, serta menyimpan log terkait perubahan dan melakukan audit log secara berkala. Setelah rilis, tim operasional Tencent Cloud melakukan verifikasi, pemantauan, dan pencatatan hasil perubahan pada lingkungan produksi.
N/A	2.4	Pengukuran Risiko terkait Pengembangan dan	(1) Pada setiap tahapan pengembangan dan pengadaan TI, Bank harus memitigasi	Pelanggan harus menerapkan proses manajemen risiko pengembangan dan pengadaan, dengan jelas menentukan faktor pengukuran risiko pengembangan dan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
		Pengadaan	risiko yang telah diidentifikasi dan diukur dengan beberapa cara pengendalian yang telah ditetapkan dalam kebijakan, standar, dan prosedur pengembangan dan pengadaan TI Bank. Setelah melakukan mitigasi, Bank harus memantau risiko yang dikendalikan dan residual risk karena setiap gangguan yang dapat mempengaruhi rencana dan proses pengembangan dan pengadaan TI, pada akhirnya dapat berdampak pada kegiatan operasional Bank. (2) Dalam rangka mengendalikan risiko terkait pengembangan TI, Bank harus dapat memastikan bahwa pengembangan sistem yang dilakukan telah sesuai dengan kebijakan, standar, dan prosedur untuk setiap tahapan	pengadaan, serta menerapkan tindakan mitigasi risiko terhadap risiko yang telah diidentifikasi. Selain itu, pelanggan juga perlu menetapkan kebijakan, standar, dan prosedur untuk setiap tahap pengembangan sistem. Jika pelanggan melakukan pengadaan sistem, maka harus menetapkan kriteria pemilihan pemasok, mengevaluasi kemampuan pemasok sebelum memilihnya, serta menandatangani perjanjian kontrak untuk memperjelas tanggung jawab dan kewajiban kedua belah pihak. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, dalam hal pengukuran dan pengendalian risiko, Tencent Cloud secara internal telah menetapkan prosedur manajemen risiko keamanan informasi. Prosedur ini secara jelas mendefinisikan aktivitas seperti identifikasi risiko, analisis risiko, penyusunan rencana penanganan risiko, serta pelacakan dan pemantauan risiko. Tencent Cloud secara berkala melakukan penilaian risiko, mengidentifikasi risiko berdasarkan skenario risiko serta alur proses bisnis, produk, atau layanan. Terhadap risiko yang telah diidentifikasi, Tencent Cloud akan mengevaluasi kemungkinan terjadinya dan tingkat dampak setiap risiko untuk menentukan tingkat risiko, serta mengambil tindakan lanjutan yang sesuai. Seluruh

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		pengembangan. (3) Dalam rangka mengendalikan risiko pada pengadaan, Bank harus membuat kriteria pemilihan vendor dan melakukan kaji ulang kemampuan vendor antara lain terkait dengan kondisi keuangan, tingkat dukungan (support level), dan pengendalian keamanan, sebelum menetapkan pilihan produk atau layanan dari vendor.	aktivitas proses ini tercatat dengan baik. Tencent Cloud juga secara berkelanjutan melakukan tindak lanjut terhadap penanganan risiko, menilai risiko residual, dan memastikan bahwa pihak yang bertanggung jawab telah mengelola risiko dengan tepat sesuai dengan persyaratan manajemen risiko Tencent Cloud. Selain itu, berdasarkan tren perubahan industri cloud dan praktik manajemen internal, Tencent Cloud secara terus-menerus memelihara dan merevisi metode penilaian risiko serta register risiko. Dalam hal pengembangan keamanan sistem, Tencent Cloud telah membangun seperangkat standar pengembangan keamanan sistem informasi internal. Tencent Cloud berupaya mengintegrasikan standar ISO/IEC 20000 Manajemen Layanan Teknologi Informasi, ISO/IEC 27001 Sistem Manajemen Keamanan Informasi, dan ISO/IEC 9001 Sistem Manajemen Mutu ke dalam seluruh siklus hidup pengembangan keamanan produk. Hal ini dilakukan dengan memperhatikan berbagai tahapan seperti analisis kebutuhan, desain, pengembangan, pengujian, penerapan, dan pemeliharaan, untuk menghilangkan masalah keamanan informasi dan privasi pada setiap tahap pengembangan produk, serta memastikan bahwa produk cloud mendapatkan pengendalian keamanan yang memadai selama

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			siklus hidupnya. Dalam aspek due diligence, Tencent Cloud akan menunjuk personel khusus untuk menanggapi kebutuhan pemeriksaan due diligence pelanggan serta menyediakan laporan audit dari pihak ketiga independen atau laporan kontrol sistem dan organisasi yang bersifat asersi sesuai permintaan pelanggan. Berikut adalah gambaran umum Tencent Cloud sebagai penyedia layanan cloud dalam berbagai aspek due diligence: • Kemampuan Profesional dan Teknis: Tencent Cloud mendemonstrasikan kemampuan teknis yang komprehensif sebagai pemimpin industri melalui teknologi komputasi awan yang kuat, kapabilitas pemrosesan data besar, penerapan kecerdasan buatan, perlindungan keamanan siber, teknologi cloud-native, tata letak pusat data global, serta solusi industri. Kemampuan teknis ini tidak hanya menjamin stabilitas dan keandalan layanan Tencent Cloud, tetapi juga menyediakan lingkungan komputasi awan yang aman dan dapat diandalkan bagi pelanggan. Kapabilitas keamanan operasional Tencent Cloud yang matang juga mampu menyediakan dukungan teknis 7*24 untuk produk-produk awan.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			Kekuatan Finansial: Sebagai merek komputasi awan yang dibangun dengan dedikasi oleh Tencent Group, Tencent Cloud mendapatkan manfaat dari kekuatan finansial yang tangguh dan kondisi keuangan yang stabil dari grup tersebut. Sejak resmi menyediakan layanan awan kepada publik pada tahun 2010, Tencent Cloud telah menunjukkan tren pertumbuhan yang signifikan dalam indikator keuangan utama seperti pendapatan dan profitabilitas. Tencent Cloud telah diakui selama empat tahun berturut-turut oleh lembaga penelitian industri terkemuka internasional Gartner, menempati posisi kedua di antara vendor China dalam dimensi kuadran strategis. Tingkat Dukungan Layanan: Pelanggan dapat memilih paket layanan yang sesuai untuk memperoleh dukungan eksklusif, yang mencakup grup dukungan khusus, manajer layanan teknis khusus, dan layanan bernilai tambah lainnya. Dalam hal kontrak dan perjanjian, Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN, General Service Level Agreement, Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. Untuk pemantauan dan evaluasi berkelanjutan pelanggan terhadap Tencent Cloud, dalam hal audit dan tinjauan pengawasan oleh pelanggan, Tencent Cloud akan bekerja sama dengan audit keamanan dan pengawasan pihak ketiga yang dilakukan pelanggan berdasarkan situasi aktual serta kesepakatan dan perjanjian dengan pelanggan. Tencent Cloud akan menyediakan personel khusus untuk memberikan bantuan, serta merespons dan mendukung secara aktif setiap aktivitas audit yang dimulai oleh pelanggan. Tencent Cloud telah memperoleh berbagai sertifikasi dan kualifikasi kepatuhan keamanan serta privasi melalui audit atau penilaian independen oleh pihak ketiga, seperti ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 22301, NIST CSF, dan SOC. Untuk memastikan kebijakan, prosedur, proses, dan langkah pengendalian teknologi informasi Tencent Cloud memenuhi persyaratan regulasi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			keuangan Indonesia, Tencent Cloud telah lolos audit kepatuhan IT industri keuangan Indonesia yang dilakukan oleh pihak ketiga independen dan sertifikasi SNI 27001. Pelanggan dapat mengunduh laporan terbaru secara mandiri dari Pusat Dokumen Kepatuhan Tencent Cloud .

5.3 Operasional Teknologi Informasi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			Pelanggan harus memastikan kelangsungan dan stabilitas operasi teknologi informasi, serta mampu mengurangi atau menurunkan risiko yang dapat mengganggu aktivitas operasional pelanggan.
12	3.2	Kebijakan, Standar, dan Prosedur terkait Aktivitas Operasional TI	Bank wajib memastikan kelangsungan dan kestabilan operasional Teknologi Informasi serta memitigasi risiko yang berpotensi dapat mengganggu kegiatan operasional Bank.	Tencent Cloud telah menetapkan standar manajemen operasional untuk memberikan panduan operasional dan persyaratan bagi perilaku operasional harian personel operasional, mencakup manajemen aset, manajemen keamanan fisik dan lingkungan, manajemen kapasitas, manajemen konfigurasi keamanan, manajemen media, dan sebagainya. Tencent Cloud menggunakan platform manajemen operasional yang matang berbasis alat dan otomatisasi untuk mengelola operasi operasional, dengan mekanisme manajemen operasional internal

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			yang mengontrol ketat jendela waktu perubahan, memastikan bahwa semua permintaan operasional dapat diselesaikan dalam waktu yang ditentukan. Tencent Cloud juga menetapkan "batas merah" keamanan operasional yang rinci dan secara berkala melakukan tinjauan keamanan operasional internal. Untuk memastikan bahwa operasi di lingkungan produksi dapat dikendalikan dan dilacak, catatan operasi operasional backend dicatat secara detail dan disimpan terpusat oleh platform log, dengan tim audit internal Tencent Cloud yang secara berkala melakukan investigasi dan pelacakan terhadap operasi mencurigakan selama proses operasional.
21	N/A	Penempatan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana	(1) Bank wajib menempatkan Sistem Elektronik pada Pusat Data dan Pusat Pemulihan Bencana di wilayah Indonesia. (2) Bank hanya dapat menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sepanjang mendapatkan persetujuan dari Otoritas Jasa Keuangan.	Pelanggan harus menempatkan sistem elektroniknya di pusat data dan pusat pemulihan bencana yang berlokasi di dalam wilayah Indonesia. Apabila pelanggan menempatkan sistem elektronik di pusat data yang berada di luar wilayah Indonesia, maka pelanggan wajib menyerahkan dokumen hukum seperti analisis risiko negara, pernyataan tertulis, dan perjanjian kerja sama untuk mendapatkan persetujuan dari Otoritas Jasa Keuangan (OJK). Tencent Cloud telah membangun atau menyewa pusat data di berbagai lokasi global sesuai dengan standar internasional terkait dan persyaratan keamanan setempat. Hal ini memberikan pelanggan pilihan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			multi-wilayah (multi-region) dan multi-zona ketersediaan (multi-availability zone), dengan tetap mematuhi ketat peraturan perundang-undangan di yurisdiksi operasi yang melindungi privasi pengguna dan keamanan data, serta secara aktif memantau perkembangan regulasi lokal. Pelanggan dapat dengan fleksibel menempatkan data dan sistem mereka di wilayah atau zona ketersediaan yang berbeda sesuai dengan kebutuhan pengembangan bisnis dan persyaratan keamanan data. Saat ini, Tencent Cloud memiliki tiga pusat data di Indonesia yang menyediakan beragam layanan komputasi awan, termasuk server awan (cloud server), basis data awan (cloud database), penyimpanan awan (cloud storage), dan lainnya. Pelanggan di Indonesia dapat memilih untuk menyimpan dan memproses data mereka secara lokal di Indonesia.
22	3.2.1	Kebijakan terkait Pusat Data	Pusat Data dan Pusat Pemulihan Bencana sebagaimana dimaksud dalam Pasal 21 wajib menjamin kelangsungan usaha Bank. a. Aktivitas Operasional Pusat Data b. Pengendalian	Pelanggan harus menetapkan kebijakan, standar, dan prosedur terkait aktivitas operasional pusat data, menerapkan kontrol akses fisik pusat data, serta melindungi keamanan lingkungan fisik pusat data guna memastikan bahwa pusat data dan pusat pemulihan bencana mampu mendukung kelangsungan operasional bisnis. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, pusat data Tencent Cloud

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
		Akses Fisik Pusat Data		tersebar di berbagai wilayah global, terdiri dari wilayah dan zona ketersediaan, yang mencakup Tiongkok Daratan, kawasan Asia Pasifik, Amerika Utara, dan Eropa. Sebagai penyedia layanan komputasi awan, Tencent Cloud berkomitmen untuk menyediakan fondasi fasilitas fisik yang aman, stabil, berkelanjutan, dan andal bagi pelanggan. Saat ini, Tencent Cloud telah mengoperasikan tiga pusat data sewaan di wilayah Indonesia. Untuk memastikan ketahanan dan keamanan pusat data, Tencent Cloud telah membangun sistem manajemen yang komprehensif dan ketat yang mencakup seluruh proses, mulai dari seleksi operator pusat data, pengaturan perjanjian, hingga pengawasan berkelanjutan. Pelanggan dapat secara fleksibel dan mandiri menempatkan data serta sistem mereka di berbagai wilayah atau zona ketersediaan yang berbeda sesuai dengan kebutuhan pengembangan bisnis dan persyaratan keamanan data, guna memenuhi kebutuhan ketahanan bencana bisnis. Setiap zona ketersediaan terhubung dengan beberapa operator jaringan di titik keluar membangun kemampuan cadangan bencana lintas wilayah pada jaringan Tencent Cloud, yang secara efektif mengurangi dampak berkelanjutan dari gangguan jaringan publik operator. Jaringan dasar Tencent Cloud mengadopsi metode konstruksi
		c. Pengendalian Lingkungan Pusat Data		

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			redundansi, yang dikombinasikan dengan teknik rekayasa lalu lintas berbasis prioritas jalur dan keterjangkauan rute pada lapisan perutean, guna memastikan bahwa layanan jaringan tidak akan terputus akibat kegagalan perangkat tunggal. Node komputasi Tencent Cloud juga dibangun dengan skema redundansi . Ketika terjadi kegagalan pada satu node komputasi, penjadwal (scheduler) akan secara otomatis dan real time mengecualikan node tersebut, sehingga secara efektif menjaga ketersediaan layanan pelanggan. Dalam proses operasional pusat data, Tencent Cloud telah membangun mekanisme pemantauan dan evaluasi rutin, yang secara berkala melakukan penilaian komprehensif terhadap lingkungan fisik, kemampuan teknis, efisiensi respons layanan, serta efektivitas pengendalian risiko dari operator pusat data. Tencent Cloud melakukan audit dan pemeriksaan onsite tahunan di pusat data untuk memverifikasi kepatuhan operator terhadap persyaratan keamanan informasi yang ditetapkan oleh Tencent Cloud. Selain itu, Tencent Cloud meninjau hasil penilaian risiko ancaman dan kerentanan yang dilaksanakan oleh operator layanan pusat data, guna memastikan efektivitas tindakan pengelolaan terkait.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				Dalam hal manajemen lingkungan fisik, semua pusat data Tencent Cloud di seluruh dunia dipilih lokasinya, dibangun, atau disewa sesuai dengan standar internasional yang relevan dan persyaratan keamanan setempat. Untuk pusat data sewaan yang diterapkan di Indonesia, Tencent Cloud mewajibkan operator pusat data untuk menggunakan sistem daya dan sistem pendingin (AC) yang sepenuhnya redundan dan berstabilitas tinggi, guna memastikan bahwa kegagalan titik tunggal apa pun tidak akan mempengaruhi kontinuitas pasokan listrik dan pendinginan pusat data. Tencent Cloud juga mewajibkan operator untuk melengkapi pusat data dengan sistem pemadam kebakaran yang lengkap, termasuk sistem deteksi kebakaran di area tertentu, sistem pemadam api otomatis, serta perangkat pemadam api manual untuk penggunaan darurat. Untuk melindungi perangkat dari kerusakan akibat listrik statis, Tencent Cloud mewajibkan operator untuk memasang rantai anti-statis di dalam pusat data dan memasang kabel pentanahan untuk kabinet, saluran kabel, dan perangkat lainnya. Dalam hal kontrol akses fisik, Tencent Cloud mewajibkan operator untuk menetapkan prosedur akses formal untuk akses fisik ke pusat data, melakukan verifikasi identitas

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			terhadap individu yang memasuki pusat data, serta memeriksa dan mencatat barang bawaan. Tencent Cloud juga mensyaratkan operator pusat data untuk secara berkala melakukan tinjauan hak akses ke pusat data guna memastikan distribusi hak akses yang tepat dan menonaktifkan hak akses yang tidak relevan atau tidak diperlukan secara tepat waktu. Untuk kunjungan eksternal ke pusat data, Tencent Cloud meminta operator untuk membangun mekanisme permohonan dan otorisasi pengunjung terkait, hanya mengizinkan pengunjung yang telah disetujui untuk mengakses area tertentu di pusat data pada waktu yang ditentukan dan didampingi oleh staf terkait. Selain itu, Tencent Cloud mensyaratkan operator untuk menetapkan prosedur persetujuan dan pemeriksaan untuk perangkat yang masuk atau keluar dari ruang server (seperti untuk instalasi, operasi, atau pemindahtanganan dan penonaktifan). Dalam hal keamanan dan pengawasan, Tencent Cloud mewajibkan personel keamanan operator pusat data untuk melakukan inspeksi harian yang ketat terhadap setiap ruang server dan kondisi peralatan sesuai dengan daftar dan rencana inspeksi, menandatangani serta mencatat waktu pemeriksaan di setiap titik pemeriksaan, dan segera

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
				mengaktifkan prosedur tanggap darurat pusat data jika ditemukan kegagalan infrastruktur atau insiden keamanan. Tencent Cloud mewajibkan operator pusat data untuk melengkapi pusat data dengan sistem alarm pemantauan video 7*24 jam tanpa titik buta, yang dijaga oleh pos keamanan, serta memastikan rekaman pengawasan disimpan secara aman untuk jangka waktu yang cukup. Untuk manajemen insiden di pusat data, Tencent Cloud mewajibkan operator pusat data untuk membangun mekanisme eskalasi insiden, rencana respons, serta prosedur penanganan, dan secara berkala melakukan simulasi dan pengujian terhadap mekanisme dan prosedur tersebut. Hal ini bertujuan memastikan kemampuan respons dan penanganan yang cepat terhadap insiden serupa, sehingga mengurangi dampak negatif dari insiden fisik dan lingkungan pusat data terhadap platform dan produk Tencent Cloud.
12	3.2.2	Kebijakan Perencanaan dan Pemantauan Kapasitas TI	Bank perlu memiliki kebijakan dan prosedur perencanaan dan pemantauan kapasitas TI untuk dapat memastikan bahwa perangkat keras dan perangkat lunak yang	Pelanggan harus membangun mekanisme perencanaan dan pemantauan kapasitas TI, secara berkelanjutan memantau penggunaan sumber daya sistem, menetapkan ambang batas kinerja dan kapasitas, serta menerapkan prosedur yang diperlukan untuk mengelola situasi yang melampaui ambang batas yang telah ditetapkan.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		digunakan Bank telah sesuai dengan kebutuhan operasional bisnis dan mengantisipasi perkembangan usaha Bank. Tanpa perencanaan kapasitas TI yang baik, Bank dapat menghadapi risiko kekurangan atau bahkan pemborosan sumber daya TI. Perencanaan kapasitas TI harus disusun untuk jangka waktu cukup panjang dan selalu dikinikan untuk mengakomodasi perubahan yang ada.	Untuk mendukung pelanggan dalam melakukan perencanaan dan penyesuaian kapasitas dengan mudah, Tencent Cloud menyediakan layanan Auto Scaling (AS). Layanan ini secara otomatis dapat memantau status kesehatan instance dan menyesuaikan sumber daya komputasi cloud server berdasarkan kebutuhan bisnis pelanggan, kebijakan yang diterapkan, serta kondisi perluasan dan pengecilan skala yang telah ditetapkan sebelumnya. Hal ini memastikan bahwa selalu tersedia jumlah instance cloud server yang sesuai untuk menangani beban aplikasi pelanggan. Untuk memantau dan mengelola kinerja sistem, pelanggan dapat menggunakan Tencent Cloud Observability Platform (TCOP). Layanan ini menyediakan pemantauan real time, analisis, dan peringatan untuk produk/layanan dan sumber daya cloud. TCOP mengumpulkan dan menampilkan melalui grafik visual berbagai metrik pemantauan yang dilaporkan secara mandiri oleh produk cloud seperti server cloud dan database cloud, serta metrik pemantauan yang dikonfigurasi khusus oleh pelanggan. Hal ini membantu pelanggan memantau secara real time tingkat penggunaan sumber daya produk cloud, kinerja aplikasi, dan status

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			operasional produk cloud. TCOP juga mendukung pengaturan peringatan berdasarkan metrik tertentu, di mana sesuai dengan aturan peringatan yang ditetapkan, notifikasi tentang anomali operasional akan dikirimkan secara tepat waktu kepada pelanggan melalui metode seperti notifikasi push pesan. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud melakukan perkiraan kebutuhan kapasitas berdasarkan kebutuhan operasional bisnis dan menyusun rencana manajemen kapasitas tahunan. Sambil memastikan kelangsungan bisnis sistem informasi, departemen bisnis melakukan perkiraan kapasitas dan menyusun perencanaan kapasitas dengan mengacu pada tren penggunaan kapasitas yang diperoleh dari pemantauan sebelumnya serta mempertimbangkan kebutuhan bisnis dan sistem baru. Dalam proses operasional sehari-hari, tim internal Tencent Cloud memantau penggunaan kapasitas layanan dukungan dasar platform cloud secara real time melalui platform pemantauan kapasitas internal, mengidentifikasi tren penggunaan kapasitas. Ketika penggunaan melebihi ambang batas yang ditetapkan, platform pemantauan akan mengirimkan peringatan kepada tim terkait untuk ditindaklanjuti dan mengambil tindakan yang diperlukan, guna

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			memastikan kelancaran operasi produk dan layanan.
12	3.2.3	Kebijakan Pengelolaan Konfigurasi Perangkat Keras dan Perangkat Lunak	Bank harus menetapkan prosedur terkait: a. proses instalasi perangkat keras dan perangkat lunak; b. pengaturan parameter (hardening) perangkat keras dan perangkat lunak; dan c. inventarisasi dan pengkinian informasi perangkat keras, perangkat lunak, infrastruktur jaringan, media penyimpan, dan perangkat pendukung lainnya yang terdapat di Pusat Data.	Pelanggan harus melakukan inventarisasi terhadap perangkat keras, infrastruktur jaringan, media penyimpanan, dan perangkat lunak, serta melakukan pembaruan secara berkala. Pelanggan juga harus menerapkan konfigurasi penguatan keamanan pada perangkat lunak dan perangkat keras. Untuk membantu pelanggan dalam melakukan manajemen aset informasi yang komprehensif, Cloud Workload Protection Platform (CWPP) Layanan ini mendukung pengumpulan otomatis asset fingerprint serta mengelola secara terpadu data asset fingerprint seperti akun, port, proses, dan aplikasi. CWPP juga mampu melakukan investigasi cepat terhadap dampak risiko insiden keamanan yang telah terjadi berdasarkan asset fingerprint, guna membantu pelanggan meningkatkan keamanan server. Pelanggan juga dapat menggunakan platform manajemen keamanan terpadu Tencent Cloud, Cloud Security Center (CSC), untuk mengelola keamanan aset informasi. CSC mencakup fungsionalitas Asset Security Center, yang membantu pelanggan dalam melakukan inventarisasi dinamis otomatis

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			terhadap aset di cloud, termasuk server cloud, penyimpanan objek, database cloud, penyeimbang beban, dan lainnya. Melalui berbagai dimensi keamanan seperti risiko konfigurasi cloud, kerentana, dan insiden keamanan, CSC menyediakan manajemen terpadu terhadap risiko keamanan aset, sehingga mengurangi risiko "IT bayangan" (shadow IT) di cloud. Cloud Security Center (CSC) juga menawarkan fungsi penilaian otomatis untuk risiko konfigurasi produk cloud, membantu pelanggan mengurangi risiko keamanan akibat kesalahan konfigurasi keamanan dalam penggunaan produk cloud, serta meningkatkan tingkat keamanan keseluruhan di lingkungan cloud. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar manajemen aset informasi dan proses manajemen siklus hidup lengkap. Hal ini mencakup pengelolaan dan perlindungan aset seperti data elektronik, perangkat keras dan perangkat virtualnya, infrastruktur, sistem aplikasi, serta perangkat lunak melalui klasifikasi dan penilaian tingkat kepentingan. Tencent Cloud mengelola perangkat keras dan komponen perangkat lunak menggunakan sistem manajemen aset, yang meliputi pendaftaran dan pengikatan aset, inventarisasi dan pembaruan informasi aset, serta pensiun dan penggantian aset.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			Tujuannya adalah untuk memastikan operasi yang stabil dari sistem dasar platform cloud dan memberikan dukungan yang andal bagi sistem bisnis. Secara bersamaan, Tencent Cloud telah membangun sistem manajemen konfigurasi dan mengelola semua komponen layanan TI serta item konfigurasi secara terpusat melalui database manajemen konfigurasi. Hal ini bertujuan untuk menstandarisasi pengelolaan item konfigurasi (CI) dan hubungan di antara mereka. Jika proses perubahan melibatkan pembaruan konfigurasi, personel operasi akan memperbarui versi dan informasi terkait item konfigurasi ke dalam database manajemen konfigurasi sesuai dengan rencana perubahan setelah perubahan selesai dilakukan. Tencent Cloud secara berkala melakukan inventarisasi aset dan mengaudit database manajemen konfigurasi untuk memastikan keabsahan, akurasi, dan kelengkapan informasi setiap item konfigurasi. Selain itu, Tencent Cloud telah membangun seperangkat standar konfigurasi keamanan jaringan dan standar baseline keamanan, yang bertujuan untuk mengelola konfigurasi keamanan perangkat jaringan, firewall, sistem operasi server host, basis data, serta sistem aplikasi secara terstandarisasi. Tencent Cloud secara terus-menerus menggunakan alat pemindaian untuk

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			mendeteksi penyimpangan konfigurasi sistem operasi, sistem manajemen basis data, dan citra virtual dari standar yang telah ditetapkan. Terhadap penyimpangan yang teridentifikasi, Tencent Cloud secara otomatis menghasilkan tiket keamanan dan mengirimkannya ke tim yang bertanggung jawab untuk diperbaiki secara tepat waktu. Tencent Cloud juga secara berkala meninjau kebijakan keamanan dan pengaturan parameter pada perangkat jaringan seperti router, firewall, dan server jaringan untuk memastikan efektivitas kebijakan dan parameter tersebut.
12	3.2.4	Kebijakan Pemeliharaan Perangkat Keras dan Perangkat Lunak	a. Pemeliharaan preventif secara berkala terhadap peralatan TI perlu dilakukan untuk meminimalisasi kegagalan pengoperasian peralatan tersebut dan untuk mendeteksi secara dini permasalahan yang potensial. Untuk itu Bank perlu memiliki perjanjian pemeliharaan dengan vendor guna memastikan ketersediaan dukungan pemeliharaan dari vendor. Pemeliharaan	Pelanggan harus melakukan pemeliharaan preventif pada perangkat TI untuk mengurangi kegagalan operasional perangkat, menandatangani perjanjian pemeliharaan dengan pemasok perangkat, serta melaksanakan kegiatan pemeliharaan sesuai jadwal. Selain itu, pelanggan juga harus memantau operasi normal perangkat lunak dan perangkat keras. Dalam hal pemeliharaan perangkat keras dan perangkat lunak Tencent Cloud yang digunakan oleh pelanggan, layanan cloud yang disediakan Tencent Cloud untuk pelanggan disampaikan berdasarkan Service Level Agreement (SLA) yang disepakati untuk setiap layanan. Indikator kinerja, standar pengukuran, serta persyaratan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		didasarkan jadwal yang telah ditetapkan, didokumentasikan pada suatu log-book, dan dilakukan kaji ulang secara berkala. b. Pemantauan terhadap perangkat keras dan perangkat lunak dilakukan setiap hari untuk memastikan seluruh perangkat tersebut beroperasi sebagaimana mestinya. Misalnya server tetap dalam keadaan menyala, kapasitas Pangkalan Data (Database) dan utilitas server tidak melampaui limit, dan fasilitas pendukung berfungsi dengan baik.	pelaporan untuk setiap layanan dijelaskan secara jelas dalam SLA setiap produk dan dipublikasikan di situs web resmi Tencent Cloud. Tencent Cloud menyediakan layanan pelanggan online dan saluran telepon melalui konsol cloud serta situs web resminya untuk mendukung pelanggan dalam memberikan umpan balik terkait masalah yang dihadapi saat menggunakan layanan Tencent Cloud. Tencent Cloud memiliki pusat layanan pelanggan dengan cadangan lintas wilayah yang mampu menangani permintaan pelanggan secara non-stop 7*24 jam, menyediakan dukungan teknis sepanjang waktu untuk produk cloud, serta respons dan penanganan layanan yang tepat waktu dan berkualitas tinggi. Pelanggan juga dapat memilih paket layanan yang sesuai untuk mendapatkan dukungan eksklusif yang terdiri dari grup dukungan khusus, manajer layanan teknis khusus, layanan bernilai tambah, dan komponen lainnya. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud menggunakan Configuration Management Database (CMDB) untuk memelihara daftar rinci perangkat keras dan fasilitas, yang mencakup tanggal akhir dukungan (End-of-Support Date) dan informasi versi platform untuk setiap server. Tencent Cloud secara berkala

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			melakukan pensiun dan penggantian server, sedangkan komponen perangkat lunak (seperti sistem operasi dan sistem basis data) diganti dengan versi yang sesuai sebelum tanggal akhir dukungan. Untuk hard disk yang telah dipensiunkan, Tencent Cloud menerapkan metode penghancuran fisik yang aman guna memastikan hard disk hancur sepenuhnya, dan mencatatnya dalam catatan penghancuran. Dalam hal pemeliharaan dan pemantauan infrastruktur, Tencent Cloud mengatur petugas di lokasi pusat data untuk secara berkala memeriksa peralatan kunci di ruang server. Mereka mencatat hasil inspeksi sesuai prosedur yang telah ditetapkan, melaporkan kondisi abnormal, dan menyelesaikan masalah yang ditemukan. Hal ini memastikan bahwa potensi risiko keamanan dapat dideteksi dan diperbaiki secara tepat waktu, sehingga menjaga stabilitas operasional peralatan. Tencent Cloud juga menerapkan sistem pemantauan yang mengawasi indikator yang telah ditetapkan untuk peralatan kunci di pusat data selama 24 jam tanpa henti. Jika terjadi kondisi abnormal, sistem secara otomatis mengirimkan peringatan kepada petugas di lokasi.
12	3.2.5	Kebijakan Manajem	Bank harus memiliki kebijakan, standar,	Pelanggan harus menetapkan prosedur manajemen perubahan, di

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
		en Perubaha n	dan prosedur manajemen perubahan yang paling sedikit mencakup permintaan, analisis, persetujuan perubahan, dan instalasi perubahan termasuk pemindahan perangkat keras dan perangkat lunak dari lingkungan pengujian ke lingkungan operasional. a. Prosedur instalasi perubahan harus memperhatikan kelangsungan operasional pada lingkungan operasional, pengawasan, dan pengaturan pengamanan sistem informasi. Standar minimal yang diatur harus mencakup risiko, pengujian, otorisasi dan persetujuan, waktu implementasi, validasi setelah penginstalan, dan back-out atau recovery. b. Dalam manajemen	mana setiap perubahan pada aset informasi harus melalui evaluasi, pengujian, tinjauan, dan persetujuan sebelum dilaksanakan. Selain itu, dalam manajemen perubahan, pelanggan harus menyimpan catatan lengkap terkait pemasangan patch. Jika sistem aplikasi pelanggan mengalami perubahan signifikan, atau perlu menggabungkan data dari beberapa sistem yang berbeda sehingga memerlukan migrasi data, pelanggan harus memiliki kebijakan, standar, dan prosedur migrasi data yang jelas. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, dalam hal manajemen perubahan, Tencent Cloud telah menetapkan seperangkat standar manajemen perubahan produk dan konfigurasi yang secara jelas menguraikan setiap langkah dalam proses perubahan serta penanggung jawab terkait. Hal ini bertujuan memastikan bahwa perubahan melalui persetujuan dan pengujian yang sesuai sebelum dilaksanakan. Secara bersamaan, Tencent Cloud mendefinisikan proses manajemen perubahan darurat, di mana perubahan darurat harus mendapatkan persetujuan yang tepat sebelum dapat dilakukan. Semua jenis perubahan program, termasuk perubahan pada aplikasi dan file konfigurasi, sistem operasi, serta basis data, harus melalui analisis

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		perubahan, Bank harus memiliki dokumentasi yang lengkap tentang instalasi patch yang dilakukan. Selain itu, Bank harus memastikan bahwa Bank menggunakan versi perangkat lunak terbaru yang paling sesuai. Bank juga harus memiliki informasi terkini mengenai perbaikan produk, masalah keamanan, patch atau upgrade, atau permasalahan lain yang sesuai dengan versi perangkat lunak yang digunakan. c. Migrasi data terjadi jika terdapat perubahan besar pada sistem aplikasi, atau terjadi penggabungan data dari beberapa sistem yang berbeda. Dalam hal terdapat migrasi data, Bank perlu memiliki kebijakan, standar, dan prosedur mengenai penanganan migrasi data.	dampak bisnis sebelum diluncurkan, menyusun rencana rollback untuk perubahan, dan mendapatkan persetujuan dari penanggung jawab terkait. Sistem rilis perubahan Tencent Cloud mewajibkan bahwa operasi perubahan hanya dapat dilakukan oleh personel yang berwenang, menyimpan log terkait perubahan, dan melakukan audit log secara berkala. Setelah perubahan dirilis, Tencent Cloud akan memvalidasi, memantau, dan mencatat hasil perubahan di lingkungan produksi. Selain itu, Tencent Cloud mengklasifikasikan tingkat dampak berdasarkan urgensi/kepentingan permintaan operasional, cakupan perubahan, dan atribut lainnya. Untuk permintaan perubahan yang berpotensi memengaruhi lingkungan eksternal, seperti produk, infrastruktur, dan konfigurasi jaringan, Tencent Cloud akan memberitahukan pelanggan melalui pengumuman, email, konsol situs web resmi Tencent Cloud, dan/atau saluran komunikasi lain yang sesuai. Dalam hal manajemen patch, Tencent Cloud akan mengidentifikasi patch terbaru dan melakukan pengujian keamanan yang memadai terhadap patch tersebut sebelum pemasangan, guna memastikan keamanan patch yang diinstal. Tencent Cloud secara berkala memberitahukan tim bisnis internal

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			untuk melakukan pemutakhiran dan pemasangan patch, serta menggunakan alat deteksi endpoint untuk memindai status pemasangan patch secara berkala. Untuk perangkat yang belum menginstal patch melebihi batas waktu yang ditetapkan, sistem akan secara otomatis menghasilkan tiket peringatan. Ketika pelanggan perlu mengakhiri perjanjian kontrak karena perubahan bisnis atau perencanaan TI di masa depan, pelanggan dapat memilih untuk melakukan pencadangan dan migrasi data cloud serta lingkungan produksi kapan saja. Tencent Cloud mendukung pelanggan dalam menggunakan format standar umum untuk mencadangkan atau memigrasikan data. Dengan demikian, pelanggan dapat menggunakan metode transfer dan protokol transfer yang sama seperti pada tahap migrasi ke cloud, atau menggunakan produk layanan Direct Connect (DC) dan VPN Connection, guna memastikan keamanan dan keandalan data selama tahap migrasi keluar dari cloud.
12	3.2.6	Kebijakan Penanganan Kejadian atau	Prosedur penanganan kejadian atau permasalahan yang baik dibutuhkan	Pelanggan harus membangun proses penanganan insiden dan masalah yang komprehensif untuk mengatasi berbagai risiko keamanan yang timbul akibat masalah tersebut.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
		Permasalahan	Bank untuk menghadapi risiko finansial, operasional, dan reputasi dari permasalahan yang timbul. Prosedur penanganan kejadian atau permasalahan harus mencakup perangkat keras, sistem operasi, sistem aplikasi, perangkat jaringan, dan peralatan keamanan. Bank harus memelihara sarana yang diperlukan untuk menangani permasalahan antara lain: a. Bank harus memiliki fungsi helpdesk agar Bank dapat menanggapi dan menangani permasalahan yang dihadapi oleh seluruh pengguna di Bank dengan segera. Bank akan menghadapi risiko jika tidak memiliki prosedur helpdesk yang memadai untuk memastikan bahwa pengguna telah memperoleh solusi	Dalam hal manajemen masalah, Tencent Cloud telah menetapkan standar manajemen masalah dengan menganalisis data dan tren insiden, mengidentifikasi akar penyebab masalah, serta mencari solusi guna meminimalkan dampak insiden dan masalah terhadap bisnis. Tencent Cloud mengelola pengetahuan penanganan masalah secara terpusat untuk meningkatkan efisiensi penanganan masalah, serta menerapkan tindakan pencegahan guna mencegah terulangnya insiden dan meningkatkan kualitas layanan. Dalam hal manajemen insiden, Tencent Cloud telah menetapkan prosedur internal untuk mengelola insiden dan permintaan layanan, serta membangun kebijakan manajemen insiden Tencent Cloud. Hal ini memastikan bahwa insiden terkait aktivitas manajemen layanan TI dicatat dan diklasifikasikan, diprioritaskan berdasarkan tingkat dampak dan urgensi, serta ditingkatkan (escalated) sesuai kebutuhan. Tujuannya adalah untuk menyelesaikan dan menutup berbagai jenis insiden dengan cepat, meminimalkan dampak insiden, menjaga kelancaran operasional bisnis, serta meningkatkan kepuasan pelanggan. Dalam hal pelanggan melaporkan masalah atau menghubungi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		atas permasalahan yang dihadapi. b. Dalam rangka penanganan permasalahan, Bank menetapkan prosedur penanganan power user agar penggunaannya tidak disalahgunakan.	Tencent Cloud secara aktif, konsol resmi Tencent Cloud menyediakan layanan tiket yang mendukung pelanggan untuk melaporkan gangguan, insiden, masalah, dan keluhan terkait keamanan, ketersediaan, dan kerahasiaan. Sistem tiket Tencent Cloud akan mengalokasikan prioritas untuk tiket pelanggan melalui mekanisme respons berjenjang. Ketika tim teknis lini pertama tidak dapat menyelesaikan masalah secara efektif, sistem secara otomatis akan memicu proses peningkatan layanan, di mana tim produk atau tim teknis akan turun tangan untuk menangani secara kolaboratif, guna memastikan kebutuhan atau umpan balik pelanggan mendapatkan respons dan penanganan yang tepat waktu. Dalam hal pelanggan melaporkan masalah atau menghubungi Tencent Cloud secara aktif, konsol resmi Tencent Cloud menyediakan layanan tiket yang mendukung pelanggan untuk melaporkan gangguan, insiden, masalah, dan keluhan terkait keamanan, ketersediaan, dan kerahasiaan. Sistem tiket Tencent Cloud akan mengalokasikan prioritas untuk tiket pelanggan melalui mekanisme respons berjenjang. Ketika tim teknis lini pertama tidak dapat menyelesaikan masalah secara efektif, sistem secara otomatis akan memicu proses peningkatan layanan, di mana tim produk atau tim teknis akan turun tangan untuk menangani

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				secara kolaboratif, guna memastikan kebutuhan atau umpan balik pelanggan mendapatkan respons dan penanganan yang tepat waktu. Tencent Cloud menyediakan layanan pelanggan online dan saluran telepon melalui konsol cloud serta situs web resminya untuk mendukung pelanggan dalam memberikan umpan balik terkait masalah yang dihadapi saat menggunakan layanan Tencent Cloud. Tencent Cloud memiliki pusat layanan pelanggan dengan cadangan lintas wilayah yang mampu menangani permintaan pelanggan secara non-stop 7*24 jam, menyediakan dukungan teknis sepanjang waktu untuk produk cloud, serta respons dan penanganan layanan yang tepat waktu dan berkualitas tinggi. Pelanggan juga dapat memilih paket layanan yang sesuai untuk mendapatkan dukungan eksklusif yang terdiri dari grup dukungan khusus, manajer layanan teknis khusus, layanan bernilai tambah, dan komponen lainnya. Dalam hal manajemen akun istimewa, Cloud Access Management (CAM) menyediakan kontrol izin yang terperinci, memberikan hak akses spesifik kepada personel berbeda untuk sumber daya yang berbeda. Pelanggan juga dapat menggunakan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			<u>CloudAudit</u> untuk memantau aktivitas akun Tencent Cloud, melakukan pemeriksaan kepatuhan, audit operasi, dan audit risiko. CloudAudit mendukung peninjauan catatan operasi konsol Tencent Cloud dan API cloud dalam 90 hari terakhir secara online. Tencent Cloud secara internal juga telah menetapkan persyaratan manajemen dan mekanisme otorisasi terkait untuk hak akses khusus. Secara bersamaan, lingkungan produksi Tencent Cloud telah sepenuhnya menerapkan bastion host, yang digunakan untuk mengontrol secara terpusat hak akses akun administrator komponen sistem backend melalui bastion host tersebut. Akses personel operasional internal ke bastion host memerlukan persetujuan otorisasi, dan hanya personel operasional internal Tencent Cloud tertentu yang dapat mengaksesnya. Login ke bastion host memerlukan autentikasi dua faktor. Catatan operasi operasional disimpan terpusat oleh platform log, dan tim audit internal Tencent Cloud secara berkala melakukan peninjauan terhadap log tersebut.
12	3.2.7	Kebijakan Pengelolaan Pangkalan Data	Bank perlu memiliki klasifikasi sensitivitas atas informasi yang disimpan pada Pangkalan Data (Database) sebagai dasar untuk	Pelanggan harus mengklasifikasikan informasi yang disimpan dalam basis data berdasarkan tingkat kepekaannya, serta menerapkan kontrol ketat pada basis data yang menyimpan informasi sensitif. Selain itu, pelanggan juga perlu menunjuk

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21		melakukan pengawasan. Pangkalan Data (Database) yang menyimpan informasi rahasia membutuhkan pengendalian yang lebih ketat dibandingkan Pangkalan Data (Database) yang menyimpan informasi yang tidak sensitif. Untuk itu, Bank memiliki fungsi Database Administrator (DBA) yang bertanggung jawab terhadap pengelolaan Pangkalan Data (Database) Bank. Prosedur yang dimiliki Bank terkait Pangkalan Data (Database) adalah pengaksesan, pemeliharaan, penanganan permasalahan, dan administrasi Pangkalan Data (Database).	administrator basis data untuk mengelola akses, pemeliharaan, dan penanganan masalah terkait basis data. Tencent Cloud menyediakan Tencent Cloud Enterprise (TCE) versi privat yang dikembangkan secara mandiri berdasarkan sistem matang Tencent Public Cloud. Layanan ini membantu pelanggan membangun fondasi digital lengkap yang otonom, terkendali, dan elastis untuk menghadapi era model besar (<i>big model era</i>), serta menyediakan solusi one-stop untuk operasi digital perusahaan. Dengan kemampuan produk yang kuat dan layanan profesional, TCE mendukung pelanggan di sektor keuangan dalam mencapai migrasi cloud yang cepat serta operasi dan pemeliharaan yang efisien. Data Security Governance Center (DSGC) dapat membantu pelanggan secara otomatis mengelola aset data, melakukan klasifikasi, serta menilai risiko keamanan data perusahaan di cloud. Layanan ini merupakan platform operasional keamanan data yang mengintegrasikan deteksi dan klasifikasi data sensitif, pemetaan data, dan analisis akses data abnormal, serta berkolaborasi dengan berbagai kemampuan keamanan Tencent Cloud untuk membentuk jaringan perlindungan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			data tertutup. Hal ini membantu perusahaan memaksimalkan manfaat keamanan. Dengan izin dari perusahaan, DSGC terhubung mendalam dengan berbagai jenis aset data di cloud, memperoleh informasi aset data secara real time dari dimensi inti. Berdasarkan karakteristik data, DSGC secara khusus membantu perusahaan mendeteksi data sensitif dan mengelola aset data dari perspektif keamanan. Sesuai standar klasifikasi data nasional, industri, atau perusahaan, DSGC membantu perusahaan melakukan klasifikasi data. Melalui visualisasi, perusahaan dapat melihat status keamanan aset dari berbagai dimensi seperti ikhtisar aset, klasifikasi data, hak akses akun, penyimpanan data, dan data sensitif. Data pelanggan di dalam Tencent Cloud dikategorikan sebagai data dengan tingkat keamanan tinggi. Kecuali untuk keperluan penyediaan layanan atau pemecahan masalah, dan setelah mendapatkan otorisasi eksplisit dari pelanggan, atau dalam situasi seperti investigasi peristiwa kriminal oleh otoritas pemerintah nasional atau lokal yang sesuai dengan peraturan perundang-undangan, karyawan internal Tencent Cloud tidak akan secara aktif mengakses data pelanggan mana pun. Selain itu, Tencent Cloud menerapkan verifikasi dan pemeliharaan identitas nyata di

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			semua node untuk hak akses data, guna menjamin integritas aset data dan keandalan layanan bisnis. Mekanisme pemantauan dan pemblokiran real time juga telah dibangun untuk mendeteksi dan mencegah setiap perilaku akses data yang tidak normal. Jaringan kantor internal Tencent Cloud sepenuhnya terisolasi dari lingkungan produksi tempat data pelanggan disimpan. Saat karyawan Tencent Cloud memperoleh persetujuan dan otorisasi pelanggan untuk mengakses aset informasi pelanggan, mereka wajib mengakses lingkungan produksi tempat data pelanggan berada melalui <i>bastion host</i> yang dilengkapi dengan autentikasi dua faktor (2FA). Saat memberikan hak akses, Tencent Cloud memastikan hanya hak akses minimum yang diperlukan untuk menyediakan layanan yang diberikan kepada karyawan melalui pembagian izin yang sangat granular. Permintaan hak akses tambahan harus melalui tinjauan dan persetujuan multi-level. Seluruh catatan operasi backend disimpan secara terpusat oleh platform log dan ditinjau secara berkala oleh tim audit internal Tencent Cloud. Secara bersamaan, untuk memastikan kerahasiaan dan integritas data pelanggan, berbagai produk penyimpanan dan basis data Tencent Cloud mendukung fungsi enkripsi data. Layanan ini menggunakan algoritma enkripsi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			yang aman dan kuat, serta mengintegrasikan <u>Key Management Service (KMS)</u> untuk mengelola siklus hidup kunci secara menyeluruh, sehingga menjamin kerahasiaan data.
12	3.2.8	Kebijakan Pengendalian Pertukaran Informasi	Bank harus memiliki prosedur pengelolaan transmisi informasi secara fisik dan logic antara lain: a. permintaan dan pemberian informasi oleh pihak intern dan ekstern; dan b. pengiriman informasi melalui berbagai media, seperti hardcopy, tape, disk, email, pos, dan internet. Pada Bank besar dengan kompleksitas TI yang tinggi, manajemen harus mempertimbangkan pemisahan segmen Wide Area Network (WAN) dan Local Area Network (LAN) dengan perangkat pengamanan seperti firewall yang membatasi akses	Pelanggan harus menetapkan proses manajemen transmisi informasi fisik dan logis, mengelola dengan baik permintaan dan penyediaan informasi internal maupun eksternal, serta transmisi informasi melalui berbagai jenis media. Untuk pelanggan bank besar dengan kompleksitas TI yang tinggi, pertimbangan dapat diberikan untuk menggunakan perangkat keamanan guna mengelola segmentasi jaringan, sehingga membatasi akses data dan lalu lintas keluar-masuk. Dalam hal perlindungan transmisi data, komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Antarmuka API cloud yang disediakan oleh produk-produk cloud Tencent Cloud juga dilengkapi dengan kemampuan keamanan seperti enkripsi HTTPS, verifikasi tanda tangan, dan pemantauan status, memberikan jaminan keamanan komunikasi pada tingkat port untuk bisnis pelanggan. Selain itu, pelanggan dapat menggunakan layanan Tencent Cloud berikut untuk mencapai transmisi data yang aman

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
			dan lalu lintas keluar masuknya data.	dalam berbagai skenario: • <u>Direct Connect (DC)</u>: Menyediakan koneksi jaringan pita lebar dengan keamanan tinggi dan khusus untuk pelanggan. Pelanggan memiliki jalur jaringan eksklusif tanpa risiko kebocoran data. • <u>VPN Connection</u>: Berdasarkan teknologi terowongan jaringan, layanan ini mewujudkan transmisi aman antara pusat data lokal dan sumber daya di Tencent Cloud. Terowongan VPN menggunakan IKE (Internet Key Exchange Protocol) dan IPsec untuk mengenkripsi data yang ditransmisikan, membangun saluran data yang aman dan terpercaya di internet, sehingga menjaga keamanan data selama proses transmisi. • <u>Cloud Connect Network (CCN)</u>: Mendukung interkoneksi jaringan internal antara VPC di cloud, serta antara VPC dan pusat data lokal (IDC), dengan kemampuan interkoneksi multipoint di seluruh jaringan, pembelajaran rute otomatis, pemilihan jalur optimal, dan konvergensi cepat saat terjadi gangguan. Semua data komunikasi dalam instance jaringan di Cloud Connect Network tidak melewati jaringan publik, sehingga menawarkan kualitas komunikasi dan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				ketersediaan jaringan yang lebih baik, serta karakteristik seperti latensi rendah dan tingkat kehilangan paket rendah. Kualitas komunikasi dijamin melalui redundansi tautan bertingkat, menjadikan transmisi data aman dan andal. Untuk pelanggan perbankan dengan kompleksitas TI yang tinggi, pelanggan dapat menggunakan layanan Virtual Private Cloud (VPC) yang disediakan oleh Tencent Cloud untuk membangun beberapa ruang jaringan independen bagi sumber daya platform cloud yang telah dibeli, serta menyesuaikan pembagian segmen jaringan, alamat IP, kebijakan perutean, dan lainnya. Layanan VPC merupakan ruang jaringan eksklusif di cloud yang dibangun berdasarkan infrastruktur Tencent Cloud. VPC menggunakan teknologi tunneling untuk membangun jaringan virtual di atas jaringan fisik dan menerapkan teknologi virtualisasi guna mencapai isolasi lengkap antara jaringan privat yang berbeda, memberikan pelanggan jaringan cloud yang aman, independen, dan terisolasi. Untuk server cloud di dalam VPC, kontrol lalu lintas masuk dan keluar pada tingkat instance dan subnet dapat diterapkan dengan mengonfigurasi aturan Security

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			Group dan Network ACL, mencapai kontrol akses jaringan pada berbagai tingkatan. Untuk menerapkan perlindungan batas jaringan guna membatasi akses data dan lalu lintas keluar-masuk, Tencent Cloud menyediakan EdgeOne (EO) platform untuk pelanggan. Berbasis pada simpul global Tencent Edge, layanan ini memberikan perlindungan keamanan dan layanan percepatan kepada pelanggan, dengan kemampuan seperti perlindungan DDoS, perlindungan Web cerdas, perlindungan serangan BOT/crawler, resolusi DNS, serta dukungan bagi pelanggan untuk mengonfigurasi aturan kontrol akses kustom sesuai kebutuhan bisnis. Pelanggan juga dapat memilih alat perlindungan batas jaringan seperti Cloud Firewall, Web Application Firewall (WAF), dan Anti-DDoS. Di antaranya, Cloud Firewall (CFW) terutama menyediakan perlindungan di berbagai batas jaringan untuk pelanggan. Layanan ini mendukung fungsi seperti kontrol aktif ACL firewall, penyaringan IPSreal time, patching virtual, dan deteksi kode berbahaya. Dengan kemampuan ini, CFW dapat memenuhi kebutuhan zona DMZ dalam jaringan tradisional, memberikan perlindungan fokus pada aset inti, serta mencapai kontrol

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			isolasi granular antar VPC. Web Application Firewall (WAF) membantu pengguna di dalam maupun di luar Tencent Cloud dalam menangani masalah keamanan situs web dan layanan web, seperti serangan web, intrusi, eksploitasi kerentanan, injeksi malware, pemalsuan, backdoor, dan serangan crawler. Sementara itu, Anti-DDoS mengatasi masalah serangan DDoS dengan memanfaatkan sumber daya perlindungan DDoS yang memadai dan berkualitas tinggi, dikombinasikan dengan algoritma pembersihan yang terus berkembang berbasis "teknologi mandiri + identifikasi cerdas AI".
12	3.2.9	Kebijakan Pengelolaan Library	Pengelola library bertanggung jawab untuk menginventarisasi dan menyimpan seluruh perangkat lunak dan data yang tersimpan dalam berbagai media, antara lain tape dan disk. Disamping itu, pengelola library juga menyimpan salinan dari seluruh kebijakan dan prosedur seperti run book manual terkait Pusat Data. Dalam membuat	Pelanggan harus menetapkan posisi administrator basis data (database administrator) yang bertanggung jawab atas inventarisasi dan penyimpanan semua perangkat lunak serta data yang tersimpan dalam berbagai media, serta menjaga dan mengelola semua kebijakan dan prosedur terkait. Selain itu, pelanggan perlu memiliki kebijakan dan prosedur untuk penyimpanan, pencadangan, dan penghapusan media. Pencadangan data dan program harus diperbarui secara berkala. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar manajemen

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			kebijakan, standar, dan prosedur untuk library, Bank harus memperhatikan kecukupan prosedur penyimpanan (storage), rekam cadang (back-up), dan pemusnahan (disposal) media. Rekam cadang (back-up) data maupun program harus selalu dikinikan agar Bank dapat memastikan kemampuannya untuk memulihkan sistem, aplikasi, dan data pada saat terjadi bencana atau gangguan lainnya.	operasional yang memberikan panduan operasional dan persyaratan bagi perilaku operasional harian personel operasional, mencakup manajemen keamanan fisik dan lingkungan, manajemen media, serta manajemen pencadangan. Dalam hal manajemen media, Tencent Cloud menyimpan dan membuang media berdasarkan tingkat kepekaan informasi yang disimpannya, serta telah menetapkan prosedur terkait manajemen media yang merinci alur kerja dan standar untuk penyimpanan dan pembuangan media. Pembuangan media harus mendapatkan persetujuan terkait terlebih dahulu, dan pencatatan yang baik harus dilakukan untuk proses pembuangannya. Bergantung pada bahan, prinsip penyimpanan, dan tingkat kepekaan informasi dari berbagai media, tim terkait akan memilih metode penanganan yang sesuai guna memastikan data tidak dapat dipulihkan dan mematuhi standar keamanan. Untuk manajemen redundansi dan pencadangan perpustakaan, untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, pusat data Tencent Cloud tersebar di berbagai wilayah global, terdiri dari wilayah dan zona ketersediaan, yang mencakup Tiongkok Daratan,

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			kawasan Asia Pasifik, Amerika Utara, dan Eropa. Sebagai penyedia layanan komputasi awan, Tencent Cloud berkomitmen untuk menyediakan fondasi fasilitas fisik yang aman, stabil, berkelanjutan, dan andal bagi pelanggan. Pelanggan dapat secara fleksibel dan mandiri menempatkan data serta sistem mereka di berbagai wilayah atau zona ketersediaan yang berbeda sesuai dengan kebutuhan pengembangan bisnis dan persyaratan keamanan data, guna memenuhi kebutuhan ketahanan bencana (disaster recovery) bisnis. Setiap zona ketersediaan terhubung dengan beberapa operator jaringan di titik keluar (network egress), membangun kemampuan cadangan bencana lintas wilayah pada jaringan Tencent Cloud, yang secara efektif mengurangi dampak berkelanjutan dari gangguan jaringan publik operator. Saat ini, Tencent Cloud memiliki tiga pusat data di Indonesia yang menyediakan berbagai layanan komputasi awan termasuk server awan, basis data awan, penyimpanan awan, dan lainnya. Pelanggan di Indonesia dapat memilih untuk menyimpan dan memproses data mereka secara lokal di Indonesia. Layanan komputasi, jaringan, penyimpanan, basis data, serta layanan kontainer dan middleware yang disediakan oleh Tencent Cloud tidak hanya menyediakan arsitektur sistem dengan ketersediaan tinggi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			bagi pelanggan, tetapi juga mendukung pelanggan dalam mengonfigurasi strategi pencadangan sistem dan data mereka sendiri, memenuhi berbagai kebutuhan pencadangan pelanggan. Dalam hal perlindungan pencadangan, untuk data pelanggan yang disimpan di cloud, Tencent Cloud menggunakan metode seperti cadangan panasreal time, penyimpanan redundan, dan pencadangan lintas wilayah untuk memastikan keamanan, keandalan, dan ketersediaan berkelanjutan dari data bisnis pelanggan yang disimpan di cloud. Tencent Cloud juga menerapkan berbagai langkah perlindungan seperti keamanan fisik, kontrol akses, dan isolasi logis, serta mendukung pelanggan dalam menggunakan Key Management Service (KMS) dan Cloud Access Management (CAM) untuk mencegah akses atau perubahan tidak sah terhadap data cadangan pelanggan.
12	3.2.10	Kebijakan Pemusnahan (Disposal) Perangkat Keras dan Perangkat Lunak	Kegiatan yang dilakukan meliputi antara lain: a. memindahkan data dari sistem produksi ke media rekam cadang (back-up) dengan	Pelanggan harus menghapus data secara tepat waktu dari perangkat lunak dan keras yang tidak lagi digunakan atau telah melewati periode retensi, memindahkan data dari sistem produksi ke media pencadangan sesuai dengan prosedur dan mekanisme yang

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		mekanisme sesuai prosedur, termasuk prosedur uji coba dan rekam cadang (back-up); b. menyimpan dokumentasi sistem sebagai persiapan jika diperlukan untuk meng-install ulang suatu sistem ke server produksi; c. mengelola arsip data sesuai masa retensi; dan d. memusnahkan data yang habis masa retensinya.	berlaku, mengarsipkan data sesuai periode retensi, serta melakukan pembuangan terhadap data yang telah melewati periode retensi. Berbagai layanan penyimpanan dan basis data yang disediakan Tencent Cloud dilengkapi dengan fungsi pencadangan, memenuhi berbagai kebutuhan pencadangan pelanggan. Contohnya: • Data yang disimpan pelanggan di Cloud Object Storage (COS) dapat disimpan secara bersamaan di beberapa wilayah yang ditentukan melalui fitur replikasi lintas wilayah. Hal ini memastikan bahwa meskipun sebagian data hilang secara tidak terduga, data lengkap masih dapat ditemukan dan dipulihkan melalui data redundan. Fitur ini juga menghindari kerugian yang dapat terjadi ketika penyimpanan di satu zona ketersediaan terkena bencana yang tidak terhindarkan, sehingga mencapai efek pencadangan multi-redundan dan pemulihan bencana lintas lokasi. • Fitur pencadangan snapshot Cloud Block Storage (CBS) data bisa dicadangkan dengan mengambil snapshot cloud disk secara tepat waktu untuk mencegah kehilangan data karena gangguan atau

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			penghapusan yang tidak disengaja serta memastikan pemulihan cepat jika terjadi kegagalan bisnis. • <u>Cloud File Storage (CFS)</u> menyediakan fungsi snapshot berkala, memudahkan pelanggan dalam menetapkan strategi tugas pencadangan secara fleksibel. • <u>Cloud Native Database</u> <u>TDSQL-C</u>, database asli cloud Tencent, mendukung dua jenis pencadangan: pencadangan logis dan pencadangan snapshot. Melalui pencadangan data lengkap serta pencadangan binlog untuk periode tertentu, seluruh kluster TDSQL-C MySQL Edition atau tabel database tertentu dapat dipulihkan ke titik waktu mana pun. • <u>TencentDB for MySQL</u> mendukung dua metode pencadangan: pencadangan otomatis dan pencadangan manual. Layanan ini juga menyediakan fungsi pencadangan lintas wilayah untuk membantu pelanggan meningkatkan kemampuan pemulihan bencana sekaligus meningkatkan keandalan data. • <u>TencentDB for MongoDB</u> menyediakan mekanisme pencadangan data otomatis dan pemulihan tanpa kehilangan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				data (lossless recovery), mendukung pencadangan data multi-node. Pelanggan dapat menyimpan data cadangan selama beberapa hari melalui mekanisme pencadangan, sehingga memudahkan pemulihan data dalam situasi bencana. Selain itu, Data Transfer Service (DTS) mendukung migrasi berbagai database relasional dan NoSQL seperti MySQL, MariaDB, PostgreSQL, Redis, MongoDB, dll. Layanan ini membantu pengguna melakukan migrasi database ke cloud dengan mudah tanpa mengganggu layanan bisnis, membangun arsitektur pemulihan bencana database berketahanan tinggi melalui salinan sinkronisasi real time, serta memenuhi kebutuhan skenario seperti penambahan data komersial dan pemisahan tugas bisnis secara asinkron melalui langganan data. Cloud Migration (CMG) mengintegrasikan berbagai alat migrasi dan menyediakan pemantauan terpadu. Selama proses migrasi, pengguna dapat memilih alat migrasi resmi dari Tencent Cloud atau alat migrasi pihak ketiga yang telah disertifikasi secara resmi. Layanan ini membantu pengguna memigrasikan sistem ke cloud dengan mudah dan cepat, serta memantau progres migrasi secara jelas. Selain itu, Tencent Cloud juga

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			menawarkan Migration Solution, yang membantu perusahaan bermigrasi ke layanan Tencent Cloud dengan biaya rendah dan efisiensi tinggi. Dengan memanfaatkan produk dan layanan cloud Tencent Cloud yang berkinerja kuat, aman, dan stabil, solusi ini mendukung operasional bisnis pelanggan. Ketika pelanggan perlu mengakhiri perjanjian kontrak karena perubahan bisnis atau perencanaan TI di masa depan, pelanggan dapat memilih untuk melakukan pencadangan dan migrasi data cloud serta lingkungan produksi kapan saja. Berdasarkan perjanjian layanan antara Tencent Cloud dengan pelanggan, jika layanan cloud telah kedaluwarsa atau diakhiri, untuk data pelanggan yang disimpan di server cloud sebagai hasil penggunaan layanan Tencent Cloud, pelanggan harus menyelesaikan migrasi data sebelum periode retensi berakhir. Tencent Cloud mendukung pelanggan dalam menggunakan format standar umum untuk mencadangkan atau memigrasikan data. Dengan demikian, pelanggan dapat menggunakan metode transfer dan protokol transfer yang sama seperti pada tahap migrasi ke cloud, atau menggunakan produk layanan Direct Connect (DC) dan VPN Connection, guna memastikan keamanan dan keandalan data selama tahap migrasi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			keluar dari cloud. Setelah layanan cloud diakhiri, Tencent Cloud akan mengikuti metode penghapusan data yang ketat dan menghapus sepenuhnya data pelanggan, termasuk salinan dan cadangannya, setelah periode retensi berakhir. Data yang telah dihapus tidak dapat dipulihkan.

5.4 Teknologi Jaringan Komunikasi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
13	4.2	Kebijakan, Standar, dan Prosedur terkait Jaringan Komunikasi	Bank wajib menyediakan jaringan komunikasi yang memenuhi prinsip kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Untuk memenuhi kewajiban tersebut, Bank harus memiliki kebijakan, standar, dan prosedur sebagai pedoman dalam menyediakan jaringan komunikasi untuk meyakinkan bahwa kelangsungan operasional dan keamanan jaringan komunikasi tetap	Pelanggan harus menyediakan jaringan komunikasi yang memenuhi prinsip kerahasiaan, integritas, dan ketersediaan, serta menetapkan kebijakan, standar, dan prosedur sebagai pedoman untuk membangun jaringan komunikasi. Jaringan dasar Tencent Cloud mengadopsi metode konstruksi redundansi, yang dikombinasikan dengan teknik rekayasa lalu lintas berbasis prioritas jalur dan keterjangkauan rute pada lapisan perutean, guna memastikan bahwa layanan jaringan tidak akan terputus akibat kegagalan perangkat tunggal. Node komputasi Tencent Cloud juga dibangun dengan skema redundansi. Ketika terjadi kegagalan pada satu node komputasi, penjadwal (scheduler) akan secara otomatis dan real time mengecualikan node

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		terjaga.	tersebut, sehingga secara efektif menjaga ketersediaan layanan pelanggan. Dalam hal keamanan komunikasi jaringan, komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Antarmuka API cloud yang disediakan oleh produk-produk cloud Tencent Cloud juga dilengkapi dengan kemampuan keamanan seperti enkripsi HTTPS, verifikasi tanda tangan, dan pemantauan status, memberikan jaminan keamanan komunikasi pada tingkat port untuk bisnis pelanggan. Direct Connect (DC) Menyediakan koneksi jaringan pita lebar dengan keamanan tinggi dan khusus untuk pelanggan. Pelanggan memiliki jalur jaringan eksklusif tanpa risiko kebocoran data. Cloud Connect Network (CCN), Mendukung interkoneksi jaringan internal antara VPC di cloud, serta antara VPC dan pusat data lokal (IDC).
13	4.3.1	Proses Manajemen Risiko Jaringan Komunikasi	Dalam mengendalikan risiko pada jaringan komunikasi, Bank harus memperhatikan hal-hal sebagai berikut: 1) Desain Jaringan Komunikasi 2) Pengendalian	Pelanggan harus merancang jaringan komunikasi dengan mempertimbangkan efisiensi dan fleksibilitas, menerapkan kontrol akses pada jaringan komunikasi, serta melaksanakan desain, operasi, dan pemeliharaan komunikasi jaringan, serta mendokumentasikan semua proses terkait. Jaringan dasar Tencent Cloud

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		Akses 3) Pengoperasian dan Pemeliharaan Jaringan Komunikasi 4) Dokumentasi.	mengadopsi metode konstruksi redundansi, yang dikombinasikan dengan teknik rekayasa lalu lintas berbasis prioritas jalur dan keterjangkauan rute pada lapisan perutean, guna memastikan bahwa layanan jaringan tidak akan terputus akibat kegagalan perangkat tunggal. Node komputasi Tencent Cloud juga dibangun dengan skema redundansi. Ketika terjadi kegagalan pada satu node komputasi, penjadwal (scheduler) akan secara otomatis dan real time mengecualikan node tersebut, sehingga secara efektif menjaga ketersediaan layanan pelanggan. Dalam hal keamanan komunikasi jaringan, komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Antarmuka API cloud yang disediakan oleh produk-produk cloud Tencent Cloud juga dilengkapi dengan kemampuan keamanan seperti enkripsi HTTPS, verifikasi tanda tangan, dan pemantauan status, memberikan jaminan keamanan komunikasi pada tingkat port untuk bisnis pelanggan. Cloud <u>Access Management (CAM)</u> membantu pelanggan mengelola akses ke produk dan sumber daya Tencent Cloud dengan aman dan terperinci. CAM juga mendukung berbagai metode verifikasi identitas dua faktor, termasuk penggunaan perangkat MFA atau kode verifikasi melalui ponsel, untuk mengonfirmasi

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				keamanan identitas dan lingkungan sebelum login dan melakukan operasi sensitif. Direct Connect (DC) Menyediakan koneksi jaringan pita lebar dengan keamanan tinggi dan khusus untuk pelanggan. Pelanggan memiliki jalur jaringan eksklusif tanpa risiko kebocoran data. Cloud Connect Network (CCN), Mendukung interkoneksi jaringan internal antara VPC di cloud, serta antara VPC dan pusat data lokal (IDC). Untuk persyaratan segmentasi jaringan, pelanggan dapat menggunakan layanan Virtual Private Cloud (VPC) yang disediakan oleh Tencent Cloud untuk membangun beberapa ruang jaringan independen bagi sumber daya platform cloud yang telah dibeli, serta menyesuaikan pembagian segmen jaringan, alamat IP, kebijakan perutean, dan lainnya. Layanan VPC merupakan ruang jaringan eksklusif di cloud yang dibangun berdasarkan infrastruktur Tencent Cloud. VPC menggunakan teknologi tunneling untuk membangun jaringan virtual di atas jaringan fisik dan menerapkan teknologi virtualisasi guna mencapai isolasi lengkap antara jaringan privat yang berbeda, memberikan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				pelanggan jaringan cloud yang aman, independen, dan terisolasi. Untuk server cloud di dalam VPC, kontrol lalu lintas masuk dan keluar pada tingkat instance dan subnet dapat diterapkan dengan mengonfigurasi aturan Security Group dan Network ACL, mencapai kontrol akses jaringan pada berbagai tingkatan. Untuk menerapkan perlindungan batas jaringan, Tencent Cloud menyediakan EdgeOne (EO) platform untuk pelanggan. Berbasis pada simpul global Tencent Edge, layanan ini memberikan perlindungan keamanan dan layanan percepatan kepada pelanggan, dengan kemampuan seperti perlindungan DDoS, perlindungan Web cerdas, perlindungan serangan BOT/crawler, resolusi DNS, serta dukungan bagi pelanggan untuk mengonfigurasi aturan kontrol akses kustom sesuai kebutuhan bisnis. Pelanggan juga dapat memilih alat perlindungan batas jaringan seperti Cloud Firewall, Web Application Firewall (WAF), dan Anti-DDoS. Di antaranya, Cloud Firewall (CFW) terutama menyediakan perlindungan di berbagai batas jaringan untuk pelanggan. Layanan ini mendukung fungsi seperti kontrol aktif ACL firewall, penyaringan IPS real time, patching virtual, dan deteksi kode

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				berbahaya. Dengan kemampuan ini, CFW dapat memenuhi kebutuhan zona DMZ dalam jaringan tradisional, memberikan perlindungan fokus pada aset inti, serta mencapai kontrol isolasi granular antar VPC. Web <u>Application Firewall (WAF)</u> membantu pengguna di dalam maupun di luar Tencent Cloud dalam menangani masalah keamanan situs web dan layanan web, seperti serangan web, intrusi, eksploitasi kerentanan, injeksi malware, pemalsuan, backdoor, dan serangan crawler. Sementara itu, Anti-DDoS mengatasi masalah serangan DDoS dengan memanfaatkan sumber daya perlindungan DDoS yang memadai dan berkualitas tinggi, dikombinasikan dengan algoritma pembersihan yang terus berkembang berbasis "teknologi mandiri + identifikasi cerdas AI". Dalam hal pengendalian dan pengelolaan keamanan jaringan, Tencent Cloud secara internal telah membangun standar manajemen keamanan jaringan dan sistem pertahanan berlapis jaringan. Melalui kebijakan dan prosedur manajemen, Tencent Cloud menetapkan standar kontrol dan perlindungan keamanan jaringan serta peran dan tanggung jawab yang sesuai, guna memastikan operasi yang aman dari layanan yang dijalankan di atas jaringan Tencent Cloud. Secara bersamaan, Tencent Cloud menerapkan arsitektur

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			keamanan jaringan yang matang, yang meliputi mekanisme perlindungan berlapis seperti firewall, sistem deteksi/pencegahan intrusi (IDS/IPS), perlindungan DDoS, isolasi logis jaringan, dan keamanan aplikasi web. Mekanisme ini secara aktif mendeteksi, menyaring, dan memblokir lalu lintas jaringan berbahaya untuk melindungi keamanan jaringan Tencent Cloud. Selain itu, Tencent Cloud menerapkan berbagai langkah seperti kontrol izin dan proses persetujuan untuk secara ketat melarang akses tidak sah ke sumber daya jaringan internal, termasuk alat analisis dan pemantauan jaringan.
13	4.3.2	Pemantau an Risiko	Pemantauan terhadap risiko yang mungkin timbul dalam jaringan komunikasi yang digunakan oleh Bank antara lain mencakup hal-hal: a. jejak audit yang tersedia harus dipantau secara teratur untuk dapat mendeteksi secara dini ada tidaknya penyimpangan; b. kinerja jaringan komunikasi diukur secara berkala berdasarkan tingkat ketersediaan (availability) dan	Pelanggan harus membangun mekanisme pemantauan risiko berkelanjutan untuk melakukan pemantauan real time terhadap potensi risiko dalam jaringan komunikasi. Langkah-langkah konkret meliputi: Melakukan peninjauan berkala terhadap catatan audit yang tersedia guna mengidentifikasi aktivitas tidak normal sedini mungkin. Terus mengukur indikator kinerja jaringan untuk memastikan stabilitas layanan. Memantau penggunaan kapasitas guna mengoptimalkan alokasi sumber daya. Serta secara proaktif mendeteksi perilaku intrusi dan serangan jaringan, serta mengambil tindakan penanganan yang tepat waktu. Dalam hal manajemen log, untuk

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			response time; c. Bank harus memantau kapasitas yang digunakan dan diperlukan untuk rencana pengembangan bisnis dibandingkan dengan kapasitas terpasang; d. Bank harus memantau dan menindaklanjuti penyusutan atau serangan terhadap jaringan komunikasi; e. Bank harus melakukan kaji ulang pemberian akses kepada pengguna secara berkala untuk meyakini bahwa akses yang diberikan masih sesuai dengan tugas dan wewenang. Selain itu, perlu dilakukan kaji ulang atas pengguna jaringan komunikasi di Bank yang memiliki akses ke jaringan komunikasi di luar Bank.	membantu pelanggan dalam mengumpulkan, mengkonsolidasi, dan menganalisis bukti terkait insiden, Tencent Cloud menyediakan <u>Cloud Log Service (CLS)</u>. CLS dirancang dengan arsitektur terdistribusi berketahanan tinggi, yang menyimpan data log dalam beberapa salinan cadangan untuk mencegah ketidaktersediaan data akibat kegagalan satu node, sehingga mencapai ketersediaan layanan yang tinggi dan memberikan jaminan layanan yang stabil serta andal untuk data log. Selain itu, <u>Elasticsearch Service (ES)</u> diimplementasikan dalam Virtual Private Cloud (VPC) yang terisolasi secara logis, memungkinkan pelanggan mengontrol penuh konfigurasi lingkungan mereka, menyesuaikan daftar kontrol akses jaringan dan grup keamanan, serta menyediakan solusi penyebaran multi-zona ketersediaan. Hal ini memastikan layanan tetap berjalan meskipun terjadi gangguan jaringan, listrik, atau force majeure lainnya di satu zona ketersediaan. Untuk pengumpulan dan penyimpanan log jaringan, <u>Cloud Firewall (CFW)</u> mendukung analisis log jaringan untuk semua lalu lintas, dengan masa penyimpanan hingga 6 bulan. Layanan ini juga mendukung analisis pelacakan ancaman tingkat

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			lanjut, yang dapat menganalisis informasi pendaftaran domain, resolusi, pencatatan (ICP), serta riwayat resolusi domain. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar dan mekanisme pengumpulan serta pengelolaan log, yang mengontrol pencatatan, ekstraksi, penyimpanan, perlindungan, analisis, dan audit berbagai jenis log seperti log masuk, log operasi, log sistem rutin, dan log insiden keamanan sistem. Tujuannya adalah untuk mendeteksi dan mencegah aktivitas sistem yang tidak normal serta potensi risiko. Semua log dikonsolidasikan ke dalam Platform Manajemen Log Tencent Cloud untuk dikelola secara terpusat, dengan menerapkan langkah-langkah pencadangan dan perlindungan ketat terhadap informasi log terkait guna mencegah modifikasi atau penghapusan tanpa izin. Tencent Cloud melakukan audit log menggunakan alat audit otomatisasi keamanan operasional dan tim audit internal untuk mendeteksi anomali sistem atau operasi, sehingga mengurangi risiko operasional. Untuk memantau dan mengelola kinerja sistem, pelanggan dapat menggunakan Tencent Cloud

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			

Observability Platform (TCOP).

Layanan ini menyediakan pemantauan real time, analisis, dan peringatan untuk produk/layanan dan sumber daya cloud. TCOP mengumpulkan dan menampilkan melalui grafik visual berbagai metrik pemantauan yang dilaporkan secara mandiri oleh produk cloud seperti server cloud dan database cloud, serta metrik pemantauan yang dikonfigurasi khusus oleh pelanggan. Hal ini membantu pelanggan memantau secara real time tingkat penggunaan sumber daya produk cloud, kinerja aplikasi, dan status operasional produk cloud. TCOP juga mendukung pengaturan peringatan berdasarkan metrik tertentu, di mana sesuai dengan aturan peringatan yang ditetapkan, notifikasi tentang anomali operasional akan dikirimkan secara tepat waktu kepada pelanggan melalui metode seperti notifikasi push pesan.

layanan cloud yang disediakan Tencent Cloud untuk pelanggan disampaikan berdasarkan Service Level Agreement (SLA) yang disepakati untuk setiap layanan. Indikator kinerja, standar pengukuran, serta persyaratan pelaporan untuk setiap layanan dijelaskan secara jelas dalam SLA setiap produk dan dipublikasikan di situs web resmi Tencent Cloud. Tencent Cloud secara berkelanjutan melacak kinerja dan ketersediaan layanan cloud, serta menyediakan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			pemantauan real time bagi pelanggan melalui konsol manajemen. Untuk mendukung pelanggan dalam memantau intrusi atau serangan jaringan komunikasi, Tencent Cloud menyediakan Threat Intelligence Center (TIX). Sebagai platform layanan intelijen terpadu, TIX menyediakan tiga kemampuan intelijen utama: intelijen dasar, intelijen permukaan serangan, dan intelijen bisnis. Platform ini mendukung fungsi seperti kueri intelijen, analisis dan penilaian IOC, serta manajemen permukaan serangan. Kemampuan ini membantu pelanggan menganalisis dan menilai insiden keamanan dengan lebih efisien, serta menilai risiko paparan aset perusahaan secara lebih komprehensif, sehingga mendukung pembangunan sistem pertahanan keamanan multidimensi yang efektif. TIX membangun jaringan titik kontak intelijen yang lengkap, mengumpulkan dan menganalisis intelijen ancaman dari berbagai sumber seperti komunitas kerentanan, lembaga keamanan, penyedia alat keamanan, media sosial, dan blog keamanan. Platform ini juga terintegrasi dengan algoritma dan daya komputasi cloud untuk menghilangkan alarm palsu, sehingga memastikan keakuratan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			intelijen. Dalam hal tinjauan berkala hak akses pengguna, Tencent Cloud memastikan bahwa hak akses tidak disalahgunakan atau digunakan secara keliru melalui penyelenggaraan audit hak akses internal secara berkala. Untuk hak akses yang tidak diperlukan lagi, tindak lanjut yang sesuai akan diambil guna mencabut hak akses yang tidak perlu secara tepat waktu.

5.5 Pengamanan Informasi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
16	5.2.1- 5.2.2	Kebijakan dan Standar Pengamanan Informasi	Manajemen Bank harus menetapkan kebijakan dan memiliki komitmen yang tinggi terhadap pengamanan informasi. Kebijakan tersebut harus sesuai dengan penerimaan risiko (risk appetite) dan dikomunikasikan secara berkala kepada seluruh pegawai Bank dan pihak ekstern yang terkait. Disamping itu, perlu dilakukan evaluasi kebijakan	Manajemen pelanggan harus menetapkan kebijakan keamanan informasi yang sesuai dengan toleransi risiko pelanggan, menunjukkan komitmen tinggi terhadap kebijakan tersebut, serta secara berkala mengomunikasikannya kepada seluruh karyawan dan pihak terkait. Selain itu, pelanggan juga perlu merujuk pada peraturan perundang-undangan dan praktik terbaik untuk menyusun standar keamanan informasi berdasarkan kebijakan keamanan informasi yang telah ditetapkan. Kebijakan keamanan informasi harus ditinjau dan diperbarui secara berkala.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		secara berkala dan apabila terdapat perubahan penting. Manajemen Bank harus menetapkan standar pengamanan informasi sesuai dengan kebijakan pengamanan informasi dengan antara lain mengacu pada ketentuan peraturan perundang-undangan dan best practice.	Guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Tim keamanan Tencent Cloud secara berkelanjutan memantau dan mengevaluasi risiko keamanan internal untuk menjaga efektivitas dan keandalan sistem manajemen keamanan informasi. Tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun, dan secara terus-menerus memantau kondisi platform cloud dan sistem internal, memastikan bahwa mereka mempertahankan postur keamanan yang baik dan mematuhi peraturan dan persyaratan standar manajemen keamanan serta peraturan perundang-undangan yang berlaku. Tencent Cloud secara

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			internal juga telah membangun mekanisme pelatihan keamanan informasi, yang menyediakan berbagai kursus pelatihan bagi karyawan. Materi pelatihan mencakup aspek-aspek seperti kesadaran keamanan dasar, keamanan kantor, identifikasi dan pertahanan kerentanan, perlindungan privasi, tanggap darurat, standar keamanan pengembangan, serta persyaratan keamanan data.
16	5.2.3.1	Prosedur Pengelolaan Aset	Prosedur pengelolaan aset meliputi paling sedikit: a. aset Bank yang terkait dengan informasi harus diidentifikasi, ditentukan pemilik atau penanggungjawabnya a, dan dicatat agar dapat dilindungi secara tepat; b. aset yang terkait dengan informasi tersebut dapat berupa data, perangkat lunak, perangkat keras, jaringan, peralatan pendukung, misalnya sumber daya listrik dan AC, dan SDM termasuk kualifikasi dan	Pelanggan harus memelihara daftar aset yang mencakup semua aset informasi serta membangun mekanisme manajemen aset informasi untuk mengidentifikasi aset, mengklasifikasikan dan menetapkan tingkatan aset, menentukan kepemilikan aset, serta melaksanakan pengelolaan keamanan sesuai dengan tingkatannya. Daftar aset harus ditinjau secara berkala dan diperbarui secara tepat waktu apabila terjadi perubahan. Pelanggan juga dapat menggunakan platform manajemen keamanan terpadu Tencent Cloud, Cloud Security Center (CSC), untuk mengelola keamanan aset informasi. CSC mencakup fungsionalitas Asset Security Center, yang membantu pelanggan dalam melakukan inventarisasi dinamis otomatis terhadap aset di cloud, termasuk

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			keterampilan; c. pengaturan penggunaan informasi dan aset harus diidentifikasi, didokumentasikan, dan diimplementasikan. Seluruh pegawai Bank dan pihak ketiga harus mematuhi pengaturan tersebut seperti pengaturan penggunaan surat elektronik, internet, mobile devices, teleworking, dan lainnya; d. informasi perlu diklasifikasikan agar dapat dilakukan pengamanan yang memadai sesuai dengan klasifikasinya.	server cloud, penyimpanan objek, database cloud, penyeimbang beban, dan lainnya. Melalui berbagai dimensi keamanan seperti risiko konfigurasi cloud, kerentana, dan insiden keamanan, CSC menyediakan manajemen terpadu terhadap risiko keamanan aset, sehingga mengurangi risiko "IT bayangan" (shadow IT) di cloud. Selain itu, Data Security Governance Center (DSGC) dapat membantu pelanggan secara otomatis mengelola aset data, melakukan klasifikasi, serta menilai risiko keamanan data perusahaan di cloud. Berdasarkan karakteristik data, DSGC secara khusus membantu perusahaan mendeteksi data sensitif dan mengelola aset data dari perspektif keamanan. Melalui visualisasi, perusahaan dapat melihat status keamanan aset dari berbagai dimensi seperti ikhtisar aset, klasifikasi data, hak akses akun, penyimpanan data, dan data sensitif. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar manajemen aset informasi dan proses manajemen siklus hidup lengkap. Hal ini mencakup pengelolaan dan perlindungan aset seperti data elektronik, perangkat keras dan perangkat virtualnya, infrastruktur, sistem aplikasi, serta perangkat lunak

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			melalui klasifikasi dan penilaian tingkat kepentingan. Tencent Cloud mengelola perangkat keras dan komponen perangkat lunak menggunakan sistem manajemen aset, yang meliputi pendaftaran dan pengikatan aset, inventarisasi dan pembaruan informasi aset, serta pensiun dan penggantian aset. Tujuannya adalah untuk memastikan operasi yang stabil dari sistem dasar platform cloud dan memberikan dukungan yang andal bagi sistem bisnis. Tencent Cloud juga menetapkan Kebijakan Penggunaan yang Dapat Diterima yang secara jelas menguraikan tanggung jawab dan kewajiban karyawan serta pihak ketiga dalam menggunakan sumber daya perusahaan Tencent Cloud (termasuk namun tidak terbatas pada sistem TI, jaringan, perangkat, dan data). Kebijakan ini mengatur perilaku penggunaan yang wajar untuk mencegah potensi risiko.
16	5.2.3.2	Prosedur Pengelolaan Sumber Daya Manusia	Prosedur pengelolaan SDM paling sedikit meliputi: a. Bank harus menerapkan pengendalian yang memadai sebelum mempekerjakan pegawai TI, konsultan, termasuk pegawai pihak penyedia jasa TI	Pelanggan harus mengelola personel yang dapat mengakses informasi secara tepat, seperti dengan membangun proses seleksi personel, menandatangani perjanjian kerahasiaan dengan karyawan, menyelenggarakan sosialisasi kesadaran risiko teknologi informasi, menetapkan tindakan penanganan pelanggaran, serta mekanisme manajemen saat terjadi pengunduran diri atau perubahan posisi. Untuk mendukung kepatuhan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		pada posisi yang memiliki kerentanan atau dampak yang besar terhadap pengamanan informasi. Sebagai contoh yaitu melakukan background check catatan kriminal atau kejahatan lainnya seperti pencurian data, dan lain-lain saat melakukan rekrutmen untuk posisi network administrator atau system administrator; b. SDM baik pegawai Bank, konsultan, pegawai honorer, dan pegawai pihak penyedia jasa TI yang memiliki akses terhadap informasi harus memahami tanggung jawab terhadap pengamanan informasi; c. peran dan tanggung jawab SDM baik pegawai Bank, konsultan, pegawai honorer, dan pegawai pihak penyedia jasa TI yang memiliki akses	pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar dan prosedur manajemen sumber daya manusia yang komprehensif, guna memastikan seleksi, perekrutan, dan penempatan personel sesuai dengan persyaratan posisi. Tencent Cloud membangun prosedur manajemen siklus hidup karyawan yang jelas, meliputi proses penerimaan, periode kerja, dan proses pemberhentian. Sebelum Penerimaan: Pelamar akan menjalani wawancara, di mana Tencent Cloud menilai apakah kompetensi mereka memenuhi persyaratan posisi. Berdasarkan hukum yang berlaku dan tingkat posisi, departemen SDM melakukan pemeriksaan latar belakang kandidat sebelum penugasan. Pemeriksaan ini mencakup riwayat pekerjaan sebelumnya, latar belakang kriminal, dan verifikasi pendidikan. Hasil pemeriksaan dicatat dalam sistem manajemen SDM Tencent Cloud. Setelah Penerimaan: Karyawan internal wajib menandatangani Perjanjian Penugasan (Assignment Agreement) dan Perjanjian Kerahasiaan (Non-Disclosure Agreement). Perjanjian Penugasan menjelaskan kebijakan keamanan yang berlaku di Tencent Cloud, serta tanggung jawab karyawan atau pihak ketiga dalam melindungi keamanan informasi dan data pribadi.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		terhadap informasi harus didefinisikan dan berdasarkan pada tingkat kebutuhan atas akses informasi serta didokumentasikan sesuai dengan kebijakan pengamanan informasi; d. dalam perjanjian dengan pegawai Bank, konsultan, pegawai honorer, dan pegawai pihak penyedia jasa TI harus tercantum ketentuan mengenai pengamanan TI yang sesuai dengan kebijakan pengamanan informasi Bank. Sebagai contoh adalah perlu adanya klausula yang menyatakan bahwa mereka harus menjaga kerahasiaan informasi yang diperolehnya sesuai dengan klasifikasi informasi; e. selain perjanjian antara Bank dengan perusahaan penyedia jasa TI, semua pegawai	Sementara Perjanjian Kerahasiaan mencakup kewajiban dan tanggung jawab kerahasiaan penandatanganan, serta konsekuensi yang mungkin diterima jika melanggar klausul kerahasiaan. Karyawan outsourcing juga harus menjalani pemeriksaan latar belakang sebelum penugasan dan tunduk pada ketentuan penugasan serta kerahasiaan yang diatur dalam perjanjian antara Tencent Cloud dan penyedia outsourcing. Persyaratan kerahasiaan antara Tencent Cloud dengan karyawan dan pihak ketiga ditinjau dan diperbarui oleh departemen hukum sesuai kebutuhan. Selama masa kerja, Tencent Cloud membangun serangkaian mekanisme pelatihan dan pembelajaran keamanan informasi untuk mendidik karyawan tentang kebijakan, prosedur, dan pedoman keamanan informasi. Karyawan wajib mengikuti pelatihan kesadaran keamanan informasi secara berkala. Proses Pemberhentian: Prosedur pemberhentian di Tencent Cloud mencakup penghentian akun dan hak akses pengguna secara tepat waktu, serta pengembalian aset perusahaan. Aset fisik Tencent Cloud dialokasikan kepada penanggung jawab yang ditetapkan dan dicatat dalam sistem pelacakan aset internal khusus Tencent Cloud. Tencent Cloud melakukan inventarisasi aset setahun sekali untuk memverifikasi keberadaan fisik aset dan mencatat

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			perusahaan penyedia jasa TI yang ditugaskan di Bank harus menandatangani suatu pernyataan menjaga kerahasiaan informasi (non-disclosure statement), termasuk kerahasiaan informasi untuk keperluan perlindungan data nasabah; f. pelatihan dan/atau sosialisasi tentang pengamanan informasi harus diberikan kepada pegawai Bank, konsultan, pegawai honorer, dan pegawai pihak penyedia jasa TI. Pelatihan dan/atau sosialisasi ini diberikan sesuai dengan peran dan tanggung jawab pegawai serta pihak penyedia jasa TI; g. Bank harus menetapkan sanksi atas pelanggaran yang dilakukan oleh SDM terhadap kebijakan pengamanan	hasilnya. Dalam Hal Tindakan Disiplin: Tencent Cloud telah menetapkan mekanisme disiplin yang menyeluruh. Setiap karyawan yang melanggar regulasi perusahaan atau terlibat dalam pengungkapan tidak sah melalui sarana apa pun akan menghadapi proses disipliner. Sesuai dengan tingkat keparahan pelanggaran, sanksi yang relevan akan diberlakukan, termasuk pemutusan kontrak kerja, gugatan hukum, dan penuntutan pidana.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		informasi; h. Bank harus menetapkan prosedur yang mengatur tentang keharusan untuk mengembalikan aset dan pengubahan atau penutupan hak akses pegawai Bank, konsultan, pegawai honorer, dan pegawai pihak penyedia jasa TI yang disebabkan karena perubahan tugas atau selesainya masa kerja atau perjanjian.	
16	5.2.3.3	Prosedur Pengamanan Fisik dan Lingkungan	Prosedur pengamanan fisik dan lingkungan paling sedikit meliputi: a. fasilitas pemrosesan informasi yang penting (misalnya mainframe, server, komputer, dan perangkat jaringan aktif) harus diberikan pengamanan secara fisik dan lingkungan yang memadai untuk mencegah akses oleh pihak tidak berwenang,	Pelanggan harus membangun mekanisme kontrol keamanan fisik dan lingkungan untuk fasilitas pemrosesan informasi, serta menerapkan prosedur perlindungan keamanan dan pemeliharaan berkala untuk perangkat keras dan infrastruktur terkait TI. Semua pusat data Tencent Cloud di seluruh dunia dipilih lokasinya, dibangun, atau disewa sesuai dengan standar internasional yang relevan dan persyaratan keamanan setempat. Untuk pusat data sewaan yang diterapkan di Indonesia, Tencent Cloud mewajibkan operator pusat data untuk menggunakan sistem daya dan sistem pendingin (AC) yang sepenuhnya redundan dan berstabilitas tinggi, guna memastikan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		kerusakan, dan gangguan lain; b. pengamanan fisik dan lingkungan terhadap fasilitas pemrosesan informasi yang penting meliputi antara lain pembatas ruangan, pengendalian akses masuk (misalnya penggunaan access control card, Personal Identification Number (PIN), dan biometrics), kelengkapan alat pengamanan di dalam ruangan, misalnya alarm, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara, dan kamera CCTV, serta pemeliharaan kebersihan ruangan dan peralatan, seperti dari debu, rokok, makanan, minuman, dan barang mudah terbakar; c. fasilitas pendukung seperti AC, sumber daya listrik, dan fire alarm	bahwa kegagalan titik tunggal apa pun tidak akan mempengaruhi kontinuitas pasokan listrik dan pendinginan pusat data. Tencent Cloud juga mewajibkan operator untuk melengkapi pusat data dengan sistem pemadam kebakaran yang lengkap, termasuk sistem deteksi kebakaran di area tertentu, sistem pemadam api otomatis, serta perangkat pemadam api manual untuk penggunaan darurat. Untuk melindungi perangkat dari kerusakan akibat listrik statis, Tencent Cloud mewajibkan operator untuk memasang lantai anti-statis di dalam pusat data dan memasang kabel pentanahan untuk kabinet, saluran kabel, dan perangkat lainnya. Dalam hal kontrol akses fisik, Tencent Cloud mewajibkan operator untuk menetapkan prosedur akses formal untuk akses fisik ke pusat data, melakukan verifikasi identitas terhadap individu yang memasuki pusat data, serta memeriksa dan mencatat barang bawaan. Tencent Cloud juga mensyaratkan operator pusat data untuk secara berkala melakukan tinjauan hak akses ke pusat data guna memastikan distribusi hak akses yang tepat dan menonaktifkan hak akses yang tidak relevan atau tidak diperlukan secara tepat waktu. Untuk kunjungan eksternal ke pusat data, Tencent Cloud meminta operator untuk membangun mekanisme permohonan dan otorisasi

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			harus dipastikan kapasitas dan ketersediaannya dalam mendukung operasional fasilitas pemrosesan informasi; d. aset milik pihak penyedia jasa TI seperti server dan switching tools harus diidentifikasi secara jelas dan diberikan perlindungan yang memadai, misalnya dengan menerapkan pengamanan yang cukup, dual control atau menempatkan secara terpisah dari aset Bank; e. pemeliharaan dan pemeriksaan secara berkala terhadap fasilitas pemrosesan informasi dan fasilitas pendukung sesuai dengan prosedur yang telah ditetapkan.	pengunjung terkait, hanya mengizinkan pengunjung yang telah disetujui untuk mengakses area tertentu di pusat data pada waktu yang ditentukan dan didampingi oleh staf terkait. Selain itu, Tencent Cloud mensyaratkan operator untuk menetapkan prosedur persetujuan dan pemeriksaan untuk perangkat yang masuk atau keluar dari ruang server (seperti untuk instalasi, operasi, atau pemindahtanganan dan penonaktifan). Dalam hal keamanan dan pengawasan, Tencent Cloud mewajibkan personel keamanan operator pusat data untuk melakukan inspeksi harian yang ketat terhadap setiap ruang server dan kondisi peralatan sesuai dengan daftar dan rencana inspeksi, menandatangani serta mencatat waktu pemeriksaan di setiap titik pemeriksaan, dan segera mengaktifkan prosedur tanggap darurat pusat data jika ditemukan kegagalan infrastruktur atau insiden keamanan. Tencent Cloud mewajibkan operator pusat data untuk melengkapi pusat data dengan sistem alarm pemantauan video 7*24 jam tanpa titik buta, yang dijaga oleh pos keamanan, serta memastikan rekaman pengawasan disimpan secara aman untuk jangka waktu yang cukup. Untuk manajemen insiden di pusat

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			data, Tencent Cloud mewajibkan operator pusat data untuk membangun mekanisme eskalasi insiden, rencana respons, serta prosedur penanganan, dan secara berkala melakukan simulasi dan pengujian terhadap mekanisme dan prosedur tersebut. Hal ini bertujuan memastikan kemampuan respons dan penanganan yang cepat terhadap insiden serupa, sehingga mengurangi dampak negatif dari insiden fisik dan lingkungan pusat data terhadap platform dan produk Tencent Cloud.
16	5.2.3.4	Prosedur Pengendalian Akses	Prosedur pengendalian akses paling sedikit meliputi: - pengendalian akses fisik dan logic; - Bank harus menerapkan metode identifikasi dan otentikasi (authentication) sesuai analisis risiko. - Bank harus memiliki prosedur formal tertulis dan telah disetujui oleh manajemen tentang pengadministrasian pengguna yang meliputi pendaftaran, perubahan dan penghapusan	Pelanggan harus membangun mekanisme autentikasi identitas dan kontrol akses untuk data serta sistem teknologi informasi guna mengelola akses ke aset informasi, serta secara berkala meninjau dan memperbarui hak akses. Dalam hal manajemen akun pengguna dan otorisasi, <u>Cloud Access Management (CAM)</u> membantu pelanggan mengelola akses ke produk dan sumber daya Tencent Cloud dengan aman dan terperinci. Pengguna dapat memodifikasi aturan kata sandi untuk sub-pengguna melalui konsol manajemen akses, termasuk kompleksitas, panjang, dan masa berlaku kata sandi. Untuk mencegah kebocoran kata sandi, Tencent Cloud menggunakan enkripsi SHA256 Hash dan penambahan Salt pada kata

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		pengguna, baik untuk pengguna intern maupun ekstern Bank, misalnya vendor atau pihak penyedia jasa TI; d. pemberian akses mengacu kepada prinsip berdasarkan kebutuhan bisnis dan dengan akses yang seminimal mungkin; e. Bank harus menetapkan prosedur pengendalian melalui pemberian password atau PIN awal (initial password atau PIN); f. Bank harus mewajibkan pengguna untuk: menjaga kerahasiaan password atau PIN; memilih password atau PIN yang berkualitas yaitu: g. Bank harus menonaktifkan hak akses bila user-id tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan password atau PIN	sandi pelanggan, sehingga menghindari penyimpanan kata sandi dalam bentuk teks biasa. CAM juga mendukung berbagai metode verifikasi identitas dua faktor, termasuk penggunaan perangkat MFA atau kode verifikasi melalui ponsel, untuk mengonfirmasi keamanan identitas dan lingkungan sebelum login dan melakukan operasi sensitif. Tencent Cloud secara internal juga menetapkan kebijakan otorisasi untuk kontrol akses dan mekanisme matriks pemisahan wewenang, yang mewajibkan akun pengguna menggunakan pengidentifikasi unik. Berdasarkan baseline keamanan, kebijakan kata sandi ditetapkan untuk akun karyawan, termasuk panjang kata sandi, kompleksitas, penguncian, dan reset. Untuk perangkat akhir, sistem operasi, aplikasi, dan perangkat jaringan internal, Tencent Cloud mengonfigurasi batas jumlah kegagalan login dan kebijakan waktu habis sesi. Tencent Cloud menggunakan sistem manajemen keamanan Zero Trust untuk mengautentikasi akses karyawan, yang mewajibkan pengguna untuk menyelesaikan autentikasi dua faktor (2FA) melalui sistem tersebut sebelum mengakses sumber daya internal. Tencent Cloud berpegang teguh pada prinsip hak istimewa paling rendah (principle of least privilege), hanya memberikan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21		(failed login attempt), dan menonaktifkan pengguna setelah mencapai jumlah maksimal kegagalan password atau PIN; h. Bank harus melakukan kaji ulang berkala oleh satuan kerja yang tidak terlibat dalam operasional pengendalian akses, terhadap hak akses pengguna untuk memastikan bahwa hak akses sesuai dengan wewenang yang diberikan; i. sistem operasi, sistem aplikasi, Pangkalan Data (Database), utility, dan perangkat lainnya yang dimiliki oleh Bank dapat membantu pelaksanaan pengamanan password atau PIN; j. Bank yang menggunakan file sharing harus menetapkan pembatasan akses paling sedikit melalui penggunaan password atau PIN	izin kepada karyawan berdasarkan tanggung jawab pekerjaan dan kebutuhan bisnis. Tinjauan izin secara berkala dilakukan untuk mencegah penyalahgunaan dan penyalahgunaan izin. Untuk pengguna dengan hak akses tinggi, pelanggan dapat menggunakan Cloud Access Management (CAM) untuk mengalokasikan izin sumber daya kepada sub-pengguna melalui metode seperti penanda (tag), guna mencapai kontrol akses terperinci terhadap sumber daya cloud. CAM juga mendukung peninjauan dan pelacakan catatan operasi karyawan melalui CloudAudit. Selain itu, Tencent Cloud menyediakan Bastion Host (BH) yang mampu mendukung otorisasi granular berdasarkan dimensi seperti pengguna, aset, akun, dan izin operasi, memastikan bahwa hak akses yang dimiliki pengguna adalah yang minimal diperlukan untuk mengakses aset dan menyelesaikan tugas kerja. Bastion Host juga mendukung fungsi audit operasi, yang mencatat dan menganalisis log operasi pengguna, sehingga memastikan jejak peristiwa keamanan dapat dilacak secara efektif.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		dan pengaturan pihak yang berwenang melakukan akses.	Tencent Cloud secara internal juga telah menetapkan persyaratan manajemen dan mekanisme otorisasi terkait untuk hak akses khusus. Secara bersamaan, lingkungan produksi Tencent Cloud telah sepenuhnya menerapkan bastion host, yang digunakan untuk mengontrol secara terpusat hak akses akun administrator komponen sistem backend melalui bastion host tersebut. Akses personel operasional internal ke bastion host memerlukan persetujuan otorisasi, dan hanya personel operasional internal Tencent Cloud tertentu yang dapat mengaksesnya. Login ke bastion host memerlukan autentikasi dua faktor.
16	5.2.3.5	Prosedur Pengamanan Operasional TI	Prosedur pengamanan operasional TI paling sedikit meliputi: a. Bank harus memelihara catatan dari versi anti virus dan perangkat lunak yang digunakan dan melakukan pemantauan informasi secara rutin tentang patch, upgrade, atau permasalahan lain yang sesuai dengan versi yang digunakan serta melakukan evaluasi, pengujian, dan instalasi hal tersebut;	Pelanggan harus menetapkan prosedur keamanan operasional TI yang mencakup manajemen patch, manajemen log, dan manajemen media fisik. Selain itu, pelanggan juga perlu secara berkala meninjau layanan operasional TI yang disediakan oleh penyedia layanan TI. Dalam hal manajemen patch, Tencent Cloud akan mengidentifikasi patch terbaru dan melakukan pengujian keamanan yang memadai terhadap patch tersebut sebelum pemasangan, guna memastikan keamanan patch yang diinstal. Tencent Cloud secara berkala memberitahukan tim bisnis internal untuk melakukan pemutakhiran dan pemasangan patch, serta menggunakan alat deteksi endpoint

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			b. Bank harus menetapkan jenis log (misalnya administrator log, user log, atau system log) serta data yang harus dimasukkan ke dalam log, jangka waktu penyimpanan dengan memperhatikan ketentuan yang berlaku, untuk membantu investigasi di masa mendatang dan pemantauan pengendalian akses; c. Bank harus melakukan kaji ulang secara berkala atas jejak audit atau log berdasarkan hasil analisis risiko baik di tingkat jaringan, sistem operasi, Pangkalan Data (Database), maupun aplikasi; d. Jejak audit atau log harus dilindungi terhadap gangguan dan akses tidak sah; e. Penunjuk waktu dari seluruh sistem elektronik Bank harus disinkronisasikan dengan sumber	untuk memindai status pemasangan patch secara berkala. Untuk perangkat yang belum menginstal patch melebihi batas waktu yang ditetapkan, sistem akan secara otomatis menghasilkan tiket peringatan. Secara bersamaan, Tencent Cloud juga membangun mekanisme pemindaian kerentanan internal dan platform pengumpulan kerentanan eksternal untuk melaporkan masalah kerentanan serta ancaman dari dalam dan luar. Tiket kerentanan keamanan dicatat dalam sistem operasi keamanan dan ditugaskan kepada penanggung jawab terkait untuk ditangani dalam waktu yang ditentukan. Selain itu, tim riset keamanan Tencent Cloud mengintegrasikan kemampuan perlindungan kerentanan ke dalam sistem Web Application Firewall (WAF) Tencent Cloud dalam bentuk patch virtual, guna memastikan keamanan menyeluruh platform komputasi awan. Untuk membantu pelanggan dalam mengumpulkan, mengkonsolidasi, dan menganalisis log, Tencent Cloud menyediakan Cloud Log Service (CLS). Sebagai platform layanan log terpadu, CLS menawarkan berbagai layanan mulai dari pengumpulan log, penyimpanan log, hingga pencarian dan analisis

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		penunjuk waktu akurat yang disepakati; f. Bank harus melakukan kaji ulang secara berkala atas layanan operasional TI yang dilakukan oleh pihak penyedia jasa TI. Periode kaji ulang harus ditetapkan dalam perjanjian kerjasama antara Bank dan pihak penyedia jasa TI; dan g. Bank harus menerapkan pengendalian media fisik dalam transit, untuk melindungi media terhadap akses yang tidak sah, penyalahgunaan, atau kerusakan selama transportasi diluar batas fisik Bank.	log, konsumsi real time, serta pengiriman log. Layanan ini membantu pelanggan menyelesaikan berbagai masalah seperti operasi bisnis, pemantauan keamanan, audit log, dan analisis log. CLS dirancang dengan arsitektur terdistribusi berketahanan tinggi, yang menyimpan data log dalam beberapa salinan cadangan untuk mencegah ketidaktersediaan data akibat kegagalan satu node, sehingga mencapai ketersediaan layanan yang tinggi dan memberikan jaminan layanan yang stabil serta andal untuk data log. Cloud Security Center (CSC) juga mendukung pengumpulan berbagai data keamanan cloud, seperti data peringatan dari produk keamanan cloud, data perubahan konfigurasi aset cloud, data perilaku operasional pengguna di cloud, serta data log dari beberapa produk cloud. Layanan ini menyediakan platform pencarian dan investigasi terpadu untuk membantu pelanggan mencapai audit dan investigasi log cloud yang komprehensif. Selain itu, Elasticsearch Service (ES) mengumpulkan dan mentransmisikan log real time dari cloud server, kontainer, serta produk cloud lainnya, atau data bisnis yang ada dan yang bertambah, ke kluster ES Tencent Cloud untuk penyimpanan terdistribusi, pencarian, dan analisis data.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud mengkonsolidasikan berbagai log seperti log masuk, log operasi, log sistem rutin, dan log insiden keamanan sistem ke dalam Platform Manajemen Log Tencent Cloud untuk dikelola secara terpusat. Langkah-langkah pencadangan dan perlindungan ketat diterapkan pada informasi log terkait guna mencegah modifikasi atau penghapusan tanpa izin. Tencent Cloud melakukan audit log menggunakan alat audit otomatisasi keamanan operasional dan tim audit internal untuk mendeteksi anomali sistem atau operasi, sehingga mengurangi risiko operasional. Tencent Cloud memastikan bahwa fasilitas terkait disinkronkan dengan sumber waktu yang akurat, dan setiap pusat data juga secara berkala memeriksa sinkronisasi waktu server NTP-nya. Untuk manajemen media fisik dalam transit, Tencent Cloud melacak seluruh proses pengeluaran, pengiriman, dan penerimaan media melalui sistem tiket (work order). Selama proses pengiriman, Tencent Cloud memilih penyedia layanan pengiriman yang aman dan andal, menerapkan langkah-langkah perlindungan sesuai tingkat kerahasiaan informasi, serta menggunakan kemasan pelindung untuk media fisik guna menghindari

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			kerusakan fisik selama pengiriman. Untuk mendukung persyaratan pengawasan outsourcing pelanggan, Tencent Cloud akan bekerja sama dengan audit keamanan dan pengawasan pihak ketiga yang dilakukan pelanggan berdasarkan situasi aktual serta kesepakatan dan perjanjian dengan pelanggan. Tencent Cloud akan menyediakan personel khusus untuk memberikan bantuan, serta merespons dan mendukung secara aktif setiap aktivitas audit yang dimulai oleh pelanggan. Selain itu, tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun dan terus memantau kondisi platform cloud serta sistem internal untuk memastikan postur keamanan yang baik, sesuai dengan ketentuan dan persyaratan peraturan perundang-undangan serta standar manajemen keamanan yang berlaku. Tencent Cloud juga menjalani audit profesional oleh pihak ketiga independen setiap tahun. Melalui laporan Sistem dan Kontrol Organisasi (SOC) yang bersifat asersi, Tencent Cloud mengungkapkan kondisi terkini pengendalian internal organisasi layanannya kepada lembaga pengguna cloud, auditor independen, regulator, pemegang saham perusahaan, serta pihak-pihak terkait lainnya. Untuk memastikan kebijakan,

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			prosedur, proses, dan langkah pengendalian teknologi informasi Tencent Cloud memenuhi persyaratan regulasi keuangan Indonesia, Tencent Cloud telah lolos audit kepatuhan IT industri keuangan Indonesia yang dilakukan oleh pihak ketiga independen dan sertifikasi SNI 27001. Pelanggan dapat mengunduh laporan terbaru secara mandiri dari Pusat Dokumen Kepatuhan Tencent Cloud.
16	5.2.3.6	Prosedur Pemantauan Pengamanan Informasi	Bank harus melakukan pemantauan dalam rangka mendeteksi upaya-upaya yang mengancam pengamanan informasi dengan metode yang ditentukan berdasarkan risiko atau tingkat kritikalitas informasi atau aset TI Bank. Pemantauan dapat dilakukan secara real time untuk memberikan alert ketika terjadi aktivitas yang tergolong mencurigakan, misalnya brute force terhadap password administrator atau upaya mengakses server pada port yang tidak wajar,	Pelanggan harus membangun kemampuan untuk mendeteksi ancaman keamanan siber, mengumpulkan, memproses, dan menganalisis informasi terkait keamanan siber yang dapat memengaruhi lingkungan bisnis dan TI. Untuk mendukung pelanggan dalam mendeteksi dan menganalisis ancaman, Tencent Cloud menyediakan Threat Intelligence Center (TIX). Sebagai platform layanan intelijen terpadu, TIX menyediakan tiga kemampuan intelijen utama: intelijen dasar, intelijen permukaan serangan, dan intelijen bisnis. Platform ini mendukung fungsi seperti kueri intelijen, analisis dan penilaian IOC, serta manajemen permukaan serangan. Kemampuan ini membantu pelanggan menganalisis dan menilai insiden keamanan dengan lebih

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		atau dilakukan secara berkala, misalnya pada akhir hari, berdasarkan tingkat risiko.	efisien, serta menilai risiko paparan aset perusahaan secara lebih komprehensif, sehingga mendukung pembangunan sistem pertahanan keamanan multidimensi yang efektif. TIX membangun jaringan titik kontak intelijen yang lengkap, mengumpulkan dan menganalisis intelijen ancaman dari berbagai sumber seperti komunitas kerentanan, lembaga keamanan, penyedia alat keamanan, media sosial, dan blog keamanan. Platform ini juga terintegrasi dengan algoritma dan daya komputasi cloud untuk menghilangkan alarm palsu, sehingga memastikan keakuratan intelijen. Selain itu, Threat Intelligence Center berfokus pada model layanan SaaS, mendukung berbagai metode pengiriman seperti API berbasis web, SDK, TIP, dan mini-program untuk memenuhi kebutuhan pelanggan yang beragam. Threat Intelligence Center juga dapat diintegrasikan dengan produk perlindungan keamanan yang sudah dimiliki pelanggan, sehingga data intelijen dari cloud dapat dikaitkan untuk meningkatkan efisiensi operasi keamanan dan respons ancaman secara keseluruhan. Berdasarkan dukungan dan pemberdayaan dari Threat Intelligence Center, Tencent Cloud berkomitmen untuk membangun sistem kemampuan keamanan pertahanan proaktif yang mencakup

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			"intelijen - serangan dan pertahanan - manajemen - perencanaan". Dengan mengintegrasikan teknologi seperti intelijen ancaman, kecerdasan buatan, dan big data, Tencent Cloud meningkatkan kemampuan dan efisiensi respons terhadap insiden keamanan. Pusat operasi keamanan 7*24 jam juga telah didirikan, yang berfokus pada deteksi, investigasi, dan respons ancaman, guna mencapai visibilitas, keterlihatan, dan kendali yang jelas atas postur keamanan.
16	5.2.3.7	Prosedur Penanganan Insiden dalam Pengamanan Informasi	Hal-hal yang harus diperhatikan Bank dalam melakukan penanganan insiden dalam pengamanan informasi antara lain sebagai berikut. a. Bank harus mengidentifikasi jenis insiden dalam pengamanan informasi misalnya pengguna dapat mengakses suatu sistem yang tidak diperbolehkan atau kelemahan (vulnerabilities) lain yang diketahui pengguna. b. Pegawai Bank, pegawai honorer, dan pegawai pihak penyedia jasa TI melaporkan setiap	Pelanggan harus menetapkan prosedur dan alur kerja untuk manajemen insiden, membentuk tim respons insiden khusus yang bertugas mencatat, menganalisis, dan melaporkan insiden keamanan. Pelanggan juga perlu secara berkala meninjau panduan penanganan insiden untuk memastikan kesesuaiannya dengan kondisi terkini perbankan. Untuk mendukung pelanggan dalam mendeteksi insiden dan merespons dengan cepat, Tencent Cloud menyediakan platform manajemen keamanan terpadu Cloud Security Center (CSC). Melalui fungsionalitas seperti Pusat Aset, Pusat Risiko, Pusat Peringatan, dan Manajemen Keamanan Tingkat Lanjut, CSC membantu pelanggan mencapai siklus operasi keamanan yang mencakup deteksi ancaman sebelum

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		kali mengetahui, menemukan, atau melihat indikasi atau potensi insiden dalam pengamanan informasi sesuai huruf a. c. Bank perlu mempertimbangkan pembentukan tim khusus yang menangani insiden pengamanan misalnya Tim Respon Insiden dalam Pengamanan Informasi (TRIPI) sesuai dengan ukuran dan kompleksitas usaha Bank. d. Bank harus menetapkan hal-hal terkait pelaporan insiden dalam pengamanan informasi sebagai. e. Bank harus menetapkan hal-hal terkait penanganan insiden dalam pengamanan informasi sebagai. f. Bank harus memelihara dokumentasi lengkap atas suatu insiden dalam pengamanan	insiden, respons dan penanganan selama insiden, serta analisis forensik pasca-insiden, sehingga meningkatkan efisiensi operasi keamanan. Dalam hal manajemen insiden, Tencent Cloud telah menetapkan prosedur internal untuk mengelola insiden dan permintaan layanan, serta membangun kebijakan manajemen insiden Tencent Cloud. Hal ini memastikan bahwa insiden terkait aktivitas manajemen layanan TI dicatat dan diklasifikasikan, diprioritaskan berdasarkan tingkat dampak dan urgensi, serta ditingkatkan (escalated) sesuai kebutuhan. Tujuannya adalah untuk menyelesaikan dan menutup berbagai jenis insiden dengan cepat, meminimalkan dampak insiden, menjaga kelancaran operasional bisnis, serta meningkatkan kepuasan pelanggan. Dalam hal komunikasi dan pemberitahuan insiden, Tencent Cloud telah menetapkan standar manajemen insiden keamanan informasi dan membangun prosedur terkait seperti respons insiden keamanan informasi, eskalasi insiden, serta pemberitahuan insiden. Hal ini bertujuan untuk memberikan peringatan atau pemberitahuan tepat waktu kepada pihak internal perusahaan, pelanggan, dan pemangku kepentingan lainnya yang

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		informasi. g. Bank secara berkala melakukan kaji ulang terhadap panduan penanganan insiden dalam pengamanan informasi untuk memastikan panduan tersebut relevan dengan kondisi sistem TI Bank terkini. h. Bank dapat mempertimbangkan pemberian insentif kepada pegawai Bank, pegawai honorer, dan pegawai pihak penyedia jasa TI yang melaporkan insiden atau vulnerabilities TI yang berisiko dieksploitasi dan mengancam pengamanan informasi, dalam rangka mendorong tercapainya pengamanan informasi yang kuat atau memadai.	mungkin atau telah terkena dampak insiden, sehingga memastikan semua pihak dapat berkomunikasi dan berkoordinasi secara tertib, cepat, dan efisien. Untuk insiden keamanan yang berpotensi memengaruhi pelanggan, Tencent Cloud akan menilai cakupan dan tingkat dampak insiden keamanan informasi, kemudian setelah melalui tinjauan internal, hasil penanganan dan analisis insiden tersebut akan disampaikan kepada pelanggan melalui saluran yang sesuai. Dukungan teknis juga akan disediakan untuk membantu pelanggan mengambil langkah perbaikan guna meminimalkan kerugian. Dalam hal pelanggan melaporkan masalah atau menghubungi Tencent Cloud secara aktif, Tencent Cloud menyediakan layanan tiket melalui konsol Tencent Cloud, yang mendukung pelanggan dalam melaporkan gangguan, insiden, masalah, dan keluhan terkait keamanan, ketersediaan, dan kerahasiaan. Selain itu, Tencent Cloud menyediakan layanan pelanggan online dan saluran telepon melalui konsol cloud serta situs web resminya untuk mendukung pelanggan dalam memberikan umpan balik terkait masalah yang dihadapi saat menggunakan layanan Tencent Cloud. Tencent Cloud memiliki pusat layanan pelanggan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			dengan cadangan lintas wilayah yang mampu menangani permintaan pelanggan secara non-stop 7*24 jam, menyediakan dukungan teknis sepanjang waktu untuk produk cloud, serta respons dan penanganan layanan yang tepat waktu dan berkualitas tinggi. Pelanggan juga dapat memilih paket layanan yang sesuai untuk mendapatkan dukungan eksklusif yang terdiri dari grup dukungan khusus, manajer layanan teknis khusus, layanan bernilai tambah, dan komponen lainnya.
N/A	5.3.1- 5.3.2	Proses Manajem en Risiko terkait Pengama nan Informasi	Bank melakukan pengukuran kecenderungan atau probabilitas terjadinya risiko terkait pengamanan informasi (ancaman mengeksploitasi kelemahan) atas setiap aset dan besarnya dampak kerugian akibat hilangnya kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) dari aset yang mungkin terjadi untuk dapat mengetahui besarnya risiko potensial yang harus dihadapi.	Pelanggan harus secara berkala mengidentifikasi ancaman dan kerentanan yang relevan dengan lingkungan TI mereka, menganalisis dan menilai risiko yang ditimbulkan oleh ancaman serta kerentanan tersebut, mengurutkan prioritas risiko, menyusun langkah-langkah mitigasi risiko, menilai risiko sisa, serta memantau efektivitas tindakan pengendalian risiko. Dalam rangka mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud secara internal menetapkan prosedur manajemen risiko keamanan informasi, yang secara jelas mendefinisikan dan memberikan panduan untuk seluruh proses manajemen risiko (identifikasi risiko, analisis risiko, penyusunan rencana penanganan risiko, serta pelacakan dan pemantauan risiko).

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		Berdasarkan hasil pengukuran risiko, Bank harus menetapkan bentuk penanganan dan pengendalian risiko yang akan diterapkan untuk meminimalisasi risiko yang dihadapi Bank. Bank dapat menganalisis kelemahan dari bentuk pengendalian yang telah diterapkan dan bentuk pengendalian pengamanan yang dapat direkomendasikan untuk diterapkan kemudian. Pengendalian intern juga dilakukan untuk memastikan bahwa pengendalian pengamanan informasi telah diterapkan, memadai, dan berjalan secara efektif sesuai dengan kebijakan, standar, dan prosedur pengamanan informasi yang berlaku.	• Identifikasi Risiko: Tencent Cloud secara berkala melaksanakan penilaian risiko, mengidentifikasi skenario risiko yang relevan berdasarkan laporan insiden keamanan industri, pengalaman praktis Tencent Cloud, serta basis data risiko dari lembaga profesional. Identifikasi risiko dilakukan melalui analisis terhadap skenario risiko serta hasil analisis proses bisnis, produk, atau layanan. • Penilaian Risiko: Tencent Cloud mengevaluasi nilai aset, kemungkinan terjadinya risiko dalam skenario tertentu, serta tingkat dampak risiko, kemudian menghitung tingkat risiko berdasarkan parameter tersebut. • Penanganan Risiko: Berdasarkan hasil analisis risiko, Tencent Cloud menerapkan strategi respons dan langkah-langkah mitigasi yang sesuai untuk setiap risiko yang teridentifikasi. Untuk risiko tinggi, penanggung jawab risiko menyusun rencana penanganan (melalui transfer risiko atau tindakan pengurangan risiko) dan memperbarui tabel manajemen risiko. Untuk risiko sedang, penanggung jawab risiko menilai kebutuhan penyusunan rencana penanganan berdasarkan kondisi aktual. Untuk risiko rendah, risiko

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			tersebut dianggap dapat diterima. Tencent Cloud juga secara berkala meninjau risiko residual untuk memantau status dan nilai risikonya. • Pemantauan, Tinjauan, dan Pelaporan Risiko: Tencent Cloud mengumpulkan hasil penilaian risiko, menghasilkan laporan penilaian risiko, dan menyampaikannya kepada manajemen. Selain itu, Tencent Cloud memelihara tabel manajemen risiko, memantau perubahan kondisi risiko serta status rencana penanganan risiko, dan menyesuaikan rencana manajemen risiko secara real time. Selain itu, Tencent Cloud mendefinisikan indikator risiko kunci dan secara berkala melakukan pengukuran terhadap indikator tersebut. Dengan membandingkannya terhadap kriteria risiko yang dapat diterima, Tencent Cloud menganalisis akar penyebab masalah yang ditemukan serta mengusulkan rekomendasi dan solusi perbaikan.

5.6 Rencana Pemulihan Bencana

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
15	6.2	Kebijakan,	(1) Bank wajib	Pelanggan harus menyusun rencana

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
		Standar, dan Prosedur terkait Rencana Pemulihan Bencana	memiliki Rencana Pemulihan Bencana. (2) Bank wajib memastikan Rencana Pemulihan Bencana sebagaimana dimaksud pada ayat (1) dapat dilaksanakan secara efektif agar kelangsungan operasional Bank tetap berjalan saat terjadi bencana dan/atau gangguan pada sarana Teknologi Informasi yang digunakan Bank. (3) Bank wajib melakukan uji coba atas Rencana Pemulihan Bencana terhadap seluruh aplikasi dan infrastruktur yang kritikal sesuai hasil analisis dampak bisnis (business impact analysis), paling sedikit 1 (satu) kali dalam 1 (satu) tahun dengan melibatkan pengguna Teknologi Informasi. (4) Bank wajib melakukan kaji ulang Rencana Pemulihan	pemulihan bencana yang komprehensif dan memastikan keberlanjutan efektivitasnya. Secara khusus, hal ini mencakup pengujian rencana pemulihan bencana untuk aplikasi dan infrastruktur kritis setidaknya setahun sekali berdasarkan hasil analisis dampak bisnis, guna memverifikasi kelayakan pelaksanaannya. Selain itu, pelanggan perlu melakukan tinjauan menyeluruh terhadap rencana tersebut setidaknya sekali setahun untuk memastikan keselarasannya dengan kebutuhan bisnis dan lingkungan teknologi, sehingga menjamin kemampuan pemulihan operasional bisnis yang cepat dan efektif jika terjadi bencana. Untuk memastikan pelanggan dapat merespons dan memulihkan fungsi kritis dengan cepat setelah terjadi bencana, berbagai produk yang disediakan Tencent Cloud memiliki karakteristik ketersediaan tinggi yang membantu pelanggan mencapai ketersediaan tinggi untuk sistem atau layanan. Contohnya: • <u>Cloud Load Balancer (CLB)</u> menyediakan layanan distribusi lalu lintas lapisan 4 dan 7 yang aman dan cepat, memperluas kapasitas layanan eksternal sistem aplikasi melalui distribusi lalu lintas, serta menghilangkan titik kegagalan tunggal. CLB diimplementasikan dengan penyebaran berbasis kluster dan secara otomatis menghapus

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun.	instance yang bermasalah, sehingga mencapai ketersediaan tinggi. • <u>Cloud Virtual Machine (CVM)</u> memiliki karakteristik ketersediaan layanan yang tinggi dan keandalan data yang tinggi. Cloud disk yang dilengkapi pada CVM menyediakan kebijakan penyimpanan tiga salinan, memastikan kemampuan migrasi dan pemulihan data yang cepat ketika salah satu salinan mengalami kegagalan. • <u>Cloud Object Storage (COS)</u> menyediakan penyimpanan data yang redundan di berbagai arsitektur dan perangkat, menawarkan fungsi pemulihan bencana lintas lokasi dan isolasi sumber daya untuk data pelanggan, sehingga mencapai daya tahan data. • <u>TencentDB for MySQL</u> mendukung keandalan data yang tinggi dan ketersediaan layanan yang tinggi, dilengkapi dengan mekanisme pencadangan otomatis data yang lengkap serta mekanisme pemulihan tanpa kehilangan data. • <u>Tencent Kubernetes Engine (TKE)</u> mengadopsi arsitektur layanan terdistribusi yang memastikan pemulihan otomatis dan migrasi cepat

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				layanan saat terjadi kegagalan; dikombinasikan dengan penyimpanan terdistribusi di backend layanan stateful, layanan ini mencapai keamanan dan ketersediaan tinggi untuk layanan dan data. Berbagai layanan penyimpanan dan basis data yang disediakan Tencent Cloud dilengkapi dengan fungsi pencadangan, memenuhi berbagai kebutuhan pencadangan pelanggan. Contohnya: • Data yang disimpan pelanggan di Cloud Object Storage (COS) dapat disimpan secara bersamaan di beberapa wilayah yang ditentukan melalui fitur replikasi lintas wilayah. Hal ini memastikan bahwa meskipun sebagian data hilang secara tidak terduga, data lengkap masih dapat ditemukan dan dipulihkan melalui data redundan. Fitur ini juga menghindari kerugian yang dapat terjadi ketika penyimpanan di satu zona ketersediaan terkena bencana yang tidak terhindarkan, sehingga mencapai efek pencadangan multi-redundan dan pemulihan bencana lintas lokasi. • Fitur pencadangan snapshot Cloud Block Storage (CBS) data bisa dicadangkan dengan mengambil snapshot cloud disk

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			secara tepat waktu untuk mencegah kehilangan data karena gangguan atau penghapusan yang tidak disengaja serta memastikan pemulihan cepat jika terjadi kegagalan bisnis. • <u>Cloud File Storage (CFS)</u> menyediakan fungsi snapshot berkala, memudahkan pelanggan dalam menetapkan strategi tugas pencadangan secara fleksibel. • <u>Cloud Native Database</u> <u>TDSQL-C</u>, database asli cloud Tencent, mendukung dua jenis pencadangan: pencadangan logis dan pencadangan snapshot. Melalui pencadangan data lengkap serta pencadangan binlog untuk periode tertentu, seluruh kluster TDSQL-C MySQL Edition atau tabel database tertentu dapat dipulihkan ke titik waktu mana pun. • <u>TencentDB for MySQL</u> mendukung dua metode pencadangan: pencadangan otomatis dan pencadangan manual. Layanan ini juga menyediakan fungsi pencadangan lintas wilayah untuk membantu pelanggan meningkatkan kemampuan pemulihan bencana sekaligus meningkatkan keandalan data.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				<u>TencentDB for MongoDB</u> menyediakan mekanisme pencadangan data otomatis dan pemulihan tanpa kehilangan data (lossless recovery), mendukung pencadangan data multi-node. Pelanggan dapat menyimpan data cadangan selama beberapa hari melalui mekanisme pencadangan, sehingga memudahkan pemulihan data dalam situasi bencana. Untuk data pelanggan yang disimpan di cloud, Tencent Cloud menggunakan metode seperti cadangan panas real time, penyimpanan redundan, dan pencadangan lintas wilayah untuk memastikan keamanan, keandalan, dan ketersediaan berkelanjutan dari data bisnis pelanggan yang disimpan di cloud. Tencent Cloud juga menerapkan berbagai langkah perlindungan seperti keamanan fisik, kontrol akses, dan isolasi logis, serta mendukung pelanggan dalam menggunakan <u>Key Management Service (KMS)</u> dan <u>Cloud Access Management (CAM)</u> untuk mencegah akses atau perubahan tidak sah terhadap data cadangan pelanggan. Tencent Cloud sepenuhnya mengisolasi berbagai wilayah (region) yang berbeda, memastikan stabilitas dan toleransi kesalahan maksimal antarwilayah.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			Untuk menjamin ketersediaan data yang tinggi, Tencent Cloud membagi setiap wilayah menjadi beberapa zona ketersediaan (availability zone) yang saling terisolasi. Desain multi-zona ketersediaan Tencent Cloud secara efektif mengurangi dampak kegagalan titik tunggal, memastikan isolasi kesalahan antar zona ketersediaan, sehingga memberikan jaminan kelangsungan bisnis bagi pelanggan. Selain itu, untuk memastikan ketersediaan berkelanjutan dari bisnis pelanggan, Tencent Cloud telah merancang dan menerapkan kerangka manajemen kelangsungan bisnis yang sesuai dengan lingkungan komputasi awannya sendiri, serta telah memperoleh sertifikasi internasional ISO/IEC 22301 untuk Sistem Manajemen Kelangsungan Bisnis. Tencent Cloud melakukan analisis dampak bisnis terhadap produk dan layanan cloud, menetapkan target waktu pemulihan (Recovery Time Objective/RTO) dan target titik data pemulihan (Recovery Point Objective/RPO) untuk setiap bisnis, serta menyusun strategi respons dan rencana kelangsungan bisnis yang berbeda berdasarkan hasil analisis dampak bisnis. Rencana pemulihan bencana yang rinci juga telah disusun untuk produk cloud dan proses kritis. Strategi, rencana, dan prosedur terkait mencakup semua aspek seperti lokasi, personel, peralatan, sistem, informasi/data, dan prioritas bisnis. Tencent Cloud

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			secara berkala melakukan uji latihan kelangsungan bisnis untuk produk cloud berdasarkan rencana kelangsungan bisnis, guna memastikan kelayakan rencana, prosedur, dan elemen lainnya. Dalam hal dukungan personel, Tencent Cloud mendefinisikan peran personel selama proses pemulihan bisnis, dengan tanggung jawab yang jelas dalam proses tersebut. Untuk keterampilan atau posisi kunci, mekanisme pelengkap peran A dan B diterapkan, serta pelatihan dan simulasi darurat dilakukan secara berkala. Hal ini bertujuan untuk memastikan pelaksanaan prosedur pemulihan yang cepat dan efektif, serta mendukung pelanggan dalam mencapai pemulihan tepat waktu dalam skenario gangguan bisnis.
15	6.3	Pengujian Rencana Pemulihan Bencana	Uji coba dilakukan atas Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun untuk seluruh sistem atau aplikasi kritikal sesuai hasil analisis dampak bisnis (business impact analysis) dan mewakili seluruh infrastruktur yang kritikal serta melibatkan pengguna TI. Jika Bank	Pelanggan harus secara berkala menguji rencana pemulihan bencana untuk memverifikasi keefektifannya. Untuk aset informasi yang dikelola oleh penyedia layanan, pelanggan perlu menilai kemampuan pemulihan bencana dari penyedia layanan dan bekerja sama dengan penyedia tersebut untuk melakukan pengujian. Pelanggan dapat menggunakan layanan Tencent Cloud Smart Advisor (TSA) untuk membantu perencanaan dan pelaksanaan uji kelangsungan bisnis. Layanan ini adalah platform tata kelola cloud yang mencakup berbagai aplikasi

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		menggunakan pihak penyedia jasa TI dalam kegiatan operasionalnya maka pengujian yang dilakukan juga perlu melibatkan pihak ekstern tersebut. Dalam hal Bank melakukan perubahan yang sangat mendasar terhadap sistem, aplikasi, atau infrastruktur TI Bank (misalnya perubahan pada core banking system) maka harus dilakukan pengujian Rencana Pemulihan Bencana paling lama 6 (enam) bulan setelah perubahan sistem dimaksud diimplementasikan.	vertikal di bidang ITOM, mengandalkan pengalaman ahli operasional berskala besar Tencent Cloud untuk mengoptimalkan infrastruktur cloud melalui tata kelola seperti pemeriksaan risiko dan simulasi kegagalan. Cloud Advisor mampu menyediakan berbagai skenario penyuntikan kegagalan dari IaaS hingga PaaS, serta template pengalaman simulasi dari berbagai industri, mencakup skenario aplikasi khas seperti pemulihan bencana lintas zona ketersediaan. Hal ini membantu pelanggan dengan cepat dan efisien menggunakan kembali solusi yang telah matang sesuai kebutuhan bisnis mereka, sehingga meningkatkan ketersediaan sistem. Untuk memastikan ketersediaan berkelanjutan dari bisnis pelanggan, Tencent Cloud menyusun strategi respons yang berbeda dan rencana kelangsungan bisnis berdasarkan hasil analisis dampak bisnis dari produk dan layanan cloud. Rencana pemulihan bencana yang rinci telah disusun untuk produk cloud dan proses kritis, di mana strategi, rencana, dan prosedur terkait mencakup semua aspek seperti lokasi, personel, peralatan, sistem, informasi/data, dan prioritas bisnis. Tencent Cloud merancang skenario uji latihan berdasarkan rencana kelangsungan bisnis, melakukan penilaian risiko uji latihan, serta menyusun langkah-langkah perlindungan yang sesuai untuk menghindari dampak negatif pada

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			layanan akibat uji latihan. Uji latihan pemulihan bencana Tencent Cloud biasanya dilakukan dengan mensimulasikan skenario pemulihan bencana klasik yang realistis, termasuk serangan dan pertahanan serta kegagalan berskala besar, guna memeriksa secara menyeluruh kemampuan pemulihan bencana, kecepatan respons, dan kapasitas pemulihan sistem. Setelah uji latihan selesai, departemen terkait perlu mengorganisir penyusunan laporan uji latihan, melakukan perbaikan berdasarkan langkah-langkah peningkatan, serta mengarsipkan dan menyimpan laporan tersebut. Jika pelanggan menilai bahwa uji latihan pemulihan bencana memerlukan keterlibatan dan kerja sama dari pihak Tencent Cloud, kami akan merespons dengan aktif dan memberikan dukungan penuh. Berdasarkan kebutuhan spesifik pelanggan, kami akan memperjelas skenario dan cakupan uji latihan, bersama-sama menyusun rencana uji latihan serta rencana pelaksanaan yang rinci, menyediakan dukungan teknis dan jaminan sumber daya yang diperlukan selama proses uji latihan, serta membantu pelanggan mengoptimalkan strategi dan proses pemulihan bencana secara berkelanjutan. Dengan demikian, kami bersama-sama meningkatkan kelangsungan bisnis dan kemampuan pemulihan bencana.
N/A	6.4	Pemelihara	Bank harus	Pelanggan harus secara berkala

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
		aan Rencana Pemulihan Bencana dan Audit Intern	melakukan pengkinian Rencana Pemulihan Bencana untuk meyakinkan kesesuaiannya dengan kondisi ekstern maupun intern. Perubahan tersebut harus dianalisis pengaruhnya terhadap Rencana Pemulihan Bencana yang ada pada saat ini dan menentukan perbaikan yang dibutuhkan untuk mengakomodasi perubahan tersebut dalam Rencana Pemulihan Bencana terbaru. Selanjutnya, Rencana Pemulihan Bencana hasil revisi tersebut harus didokumentasikan dan didistribusikan kepada satuan kerja TI. Auditor Intern harus melakukan pemeriksaan terhadap: a. kesesuaian Rencana Pemulihan Bencana dengan kebijakan manajemen risiko Bank;	memperbarui rencana pemulihan bencana untuk memastikan kesesuaiannya dengan lingkungan internal dan eksternal perusahaan, serta secara rutin melakukan audit internal terhadap rencana pemulihan bencana. Hal ini bertujuan memastikan keselarasan dengan kebijakan manajemen risiko perusahaan, mencakup aktivitas kunci dalam hasil analisis dampak bisnis, dan melaporkan temuan serta laporan audit yang signifikan secara tepat waktu. Tencent Cloud melakukan evaluasi tahunan terhadap kelengkapan, kelayakan, dan efektivitas sistem manajemen kelangsungan bisnis, serta merevisi sistem tersebut berdasarkan hasil evaluasi. Tencent Cloud juga meninjau rencana kelangsungan bisnis setiap tahun dan memperbarui rencana sesuai kebutuhan berdasarkan hasil tinjauan. Ketika terjadi perubahan signifikan dalam fungsi bisnis atau sumber daya kunci, Tencent Cloud akan meninjau cakupan bisnis dan fungsi kritis serta ketergantungan komponen masing-masing, serta merevisi rencana kelangsungan bisnis secara tepat waktu. Tencent Cloud secara berkala meminta pihak ketiga untuk melakukan audit terhadap pelaksanaan manajemen kelangsungan bisnis, guna memastikan pemenuhan persyaratan sistem manajemen kelangsungan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		b. Rencana Pemulihan Bencana mencakup kegiatan kritikal berdasarkan analisis dampak bisnis (business impact analysis) yang telah dilakukan oleh Bank; c. kecukupan Rencana Pemulihan Bencana untuk mengendalikan dan memitigasi risiko yang telah ditetapkan dalam risk assessment; d. kecukupan prosedur pengujian Rencana Pemulihan Bencana; e. efektifitas pelaksanaan pengujian Rencana Pemulihan Bencana; f. keterkinian Rencana Pemulihan Bencana sesuai perkembangan kegiatan operasional Bank dan hasil pengujian terakhir. Auditor intern harus mengomunikasikan hasil pemeriksaan dan memberikan rekomendasi kepada Direksi. Direksi	bisnis ISO 22301. Untuk ketidaksesuaian yang ditemukan dalam audit, Tencent Cloud akan menganalisis penyebab aktual atau potensial secara tepat waktu, menilai kebutuhan dan prioritas tindakan korektif dan pencegahan, serta menerapkan tindakan tersebut setelah mendapatkan persetujuan yang relevan. Efektivitas pelaksanaan tindakan korektif akan terus dilacak dan dicatat.

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		hendaknya melakukan kaji ulang atas laporan hasil audit tersebut dan merencanakan penyempurnaan atau perbaikan.	

5.7 Audit Intern

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
19	8.2-8.3	Kebijakan, Standar, dan Prosedur terkait Audit TI	(1) Bank wajib memiliki pedoman audit intern atas penggunaan Teknologi Informasi yang diselenggarakan oleh Bank sendiri dan/atau oleh pihak penyedia jasa Teknologi Informasi. (2) Bank wajib melakukan kaji ulang atas fungsi audit intern atas penggunaan Teknologi Informasi paling sedikit 1 (satu) kali dalam 3 (tiga) tahun. (3) Kaji ulang sebagaimana dimaksud pada ayat (2) wajib	Pelanggan harus menetapkan mekanisme audit internal untuk penggunaan teknologi informasi, dengan audit fungsi audit internal teknologi informasi dilakukan oleh pihak ketiga independen setidaknya sekali setiap tiga tahun. Pelanggan juga harus menyampaikan hasil audit internal dan eksternal kepada Otoritas Jasa Keuangan. Tim keamanan Tencent Cloud secara berkelanjutan melakukan pemantauan dan penilaian terhadap risiko keamanan internal untuk memastikan efektivitas dan keandalan sistem manajemen keamanan informasi. Selain itu, tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun dan terus memantau kondisi platform cloud serta sistem internal untuk memastikan postur keamanan yang baik, sesuai dengan ketentuan dan persyaratan peraturan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		menggunakan jasa pihak ekstern yang independen. (4) Bank wajib menyampaikan kepada Otoritas Jasa Keuangan: a. hasil kaji ulang sebagaimana dimaksud pada ayat (3) disertai saran perbaikan sebagai bagian dari laporan kaji ulang; dan b. hasil audit intern terhadap Teknologi Informasi sebagai bagian dari laporan pelaksanaan dan pokok-pokok hasil audit intern, sebagaimana diatur dalam ketentuan mengenai penerapan standar pelaksanaan fungsi audit intern.	perundang-undangan serta standar manajemen keamanan yang berlaku. Tencent Cloud juga menjalani audit profesional oleh pihak ketiga independen setiap tahun. Melalui laporan Sistem dan Kontrol Organisasi (SOC) yang bersifat asersi, Tencent Cloud mengungkapkan kondisi terkini pengendalian internal organisasi layanannya kepada lembaga pengguna cloud, auditor independen, regulator, pemegang saham perusahaan, serta pihak-pihak terkait lainnya. Untuk memastikan kebijakan, prosedur, proses, dan langkah pengendalian teknologi informasi Tencent Cloud memenuhi persyaratan regulasi keuangan Indonesia, Tencent Cloud telah lolos audit kepatuhan IT industri keuangan Indonesia yang dilakukan oleh pihak ketiga independen dan sertifikasi SNI 27001. Pelanggan dapat mengunduh laporan terbaru secara mandiri dari Pusat Dokumen Kepatuhan Tencent Cloud. Tencent Cloud akan secara aktif mendukung persyaratan manajemen outsourcing pelanggan, serta responsif dan kooperatif dalam menghadapi audit atau kegiatan penilaian yang dimulai oleh pihak pelanggan.

5.8 Penggunaan Pihak Penyedia Jasa TI

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		(1) Bank menyelenggarakan Teknologi Informasi. (2) Penyelenggaraan Teknologi Informasi sebagaimana dimaksud pada ayat (1) dapat dilakukan oleh Bank sendiri dan/atau pihak penyedia jasa Teknologi Informasi. (3) Dalam hal penyelenggaraan Teknologi Informasi Bank dilakukan oleh pihak penyedia jasa Teknologi Informasi sebagaimana dimaksud pada ayat (2), Bank wajib: a. bertanggung jawab atas penerapan manajemen risiko; b. memiliki satuan kerja Teknologi Informasi; c. memiliki pejabat tertinggi yang memimpin satuan kerja Teknologi Informasi; d. mampu melakukan pengawasan atas pelaksanaan kegiatan Bank yang	Jika operasional teknologi informasi pelanggan dilaksanakan oleh penyedia layanan teknologi informasi, pelanggan harus membangun proses penggunaan penyedia layanan TI eksternal. Proses ini mencakup penyampaian kebutuhan, pengiriman permintaan proposal kepada penyedia layanan TI, pelaksanaan due diligence, penandatanganan perjanjian kontrak dengan penyedia layanan TI, serta kesepakatan klausul khusus. Selain itu, pelanggan harus memastikan bahwa penyedia layanan TI memberikan hak akses data dan informasi ketika diperlukan dalam audit internal, eksternal, atau oleh regulator. Dalam aspek due diligence, Tencent Cloud akan menunjuk personel khusus untuk menanggapi kebutuhan pemeriksaan due diligence pelanggan serta menyediakan laporan audit dari pihak ketiga independen atau laporan kontrol sistem dan organisasi yang bersifat asersi sesuai permintaan pelanggan. Berikut adalah gambaran umum Tencent Cloud sebagai penyedia layanan cloud dalam berbagai aspek due diligence: • Reputasi dan Pengalaman Industri: Sebagai merek komputasi awan di bawah Tencent, pemimpin industri internet Tiongkok, Tencent Cloud
20	9.2	Kebijakan, Standar, dan Prosedur Penggunaan Penyedia Jasa TI		

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		diselenggarakan oleh pihak penyedia jasa; e. memilih pihak penyedia jasa Teknologi Informasi berdasarkan analisa biaya dan manfaat (cost and benefit analysis) dengan mengikutsertakan satuan kerja Teknologi Informasi Bank; f. memantau dan mengevaluasi keandalan pihak penyedia jasa Teknologi Informasi secara berkala yang menyangkut kinerja, reputasi penyedia jasa, dan kelangsungan penyediaan layanan; g. memberikan akses kepada auditor intern, auditor ekstern, dan Otoritas Jasa Keuangan untuk memperoleh data dan informasi setiap kali dibutuhkan; h. memberikan akses kepada Otoritas Jasa Keuangan terhadap Pangkalan Data secara tepat waktu, baik untuk data	telah memperoleh berbagai sertifikasi profesional dari lembaga industri, menyediakan solusi komputasi awan yang komprehensif, serta telah melayani banyak perusahaan dan institusi pemerintah dengan layanan komputasi awan yang andal, diakui oleh pelanggan dari berbagai industri global. • Tenaga Profesional: Tencent Cloud mendirikan Komite Teknologi Keamanan serta tim keamanan profesional dengan fungsi dan bidang keahlian yang berbeda-beda, serta menghimpun tim layanan ahli berpengalaman di industri. Hal ini bertujuan menyediakan produk dan layanan yang aman, andal, profesional, dan sesuai regulasi bagi pelanggan. • Kemampuan Profesional dan Teknis: Tencent Cloud mendemonstrasikan kemampuan teknis yang komprehensif sebagai pemimpin industri melalui teknologi komputasi awan yang kuat, kapabilitas pemrosesan data besar, penerapan kecerdasan buatan, perlindungan keamanan siber, teknologi cloud-native, tata letak pusat data global, serta solusi industri. Kemampuan teknis ini tidak hanya menjamin stabilitas dan keandalan layanan Tencent Cloud, tetapi juga menyediakan lingkungan komputasi awan yang aman dan dapat diandalkan bagi pelanggan. Kapabilitas keamanan operasional

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			terkini maupun untuk data yang telah lalu; dan i. memastikan pihak penyedia jasa Teknologi Informasi: - memiliki tenaga ahli yang memiliki keandalan dengan didukung oleh sertifikat keahlian secara akademis dan/atau secara profesional sesuai dengan keperluan penyelenggaraan Teknologi Informasi; - menerapkan prinsip pengendalian Teknologi Informasi (Information Technology control) secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen; - menyediakan akses bagi auditor intern Bank, auditor ekstern yang ditunjuk oleh Bank, Otoritas Jasa Keuangan, dan/atau pihak lain yang sesuai dengan ketentuan peraturan perundang-undangan	Tencent Cloud yang matang juga mampu menyediakan dukungan teknis 7*24 untuk produk-produk awan. Kapabilitas dan Skala Operasional: Kapabilitas dan skala operasional Tencent Cloud berada di posisi terdepan dalam industri. Pusat data Tencent Cloud tersebar di berbagai wilayah global, mencakup Tiongkok Daratan, Asia Pasifik, Amerika Utara, dan Eropa. Tencent Cloud telah bekerja sama dengan lebih dari 11.000 mitra, menyediakan lebih dari 400 solusi industri untuk klien perusahaan di lebih dari 30 sektor. Kekuatan Finansial: Sebagai merek komputasi awan yang dibangun dengan dedikasi oleh Tencent Group, Tencent Cloud mendapatkan manfaat dari kekuatan finansial yang tangguh dan kondisi keuangan yang stabil dari grup tersebut. Sejak resmi menyediakan layanan awan kepada publik pada tahun 2010, Tencent Cloud telah menunjukkan tren pertumbuhan yang signifikan dalam indikator keuangan utama seperti pendapatan dan profitabilitas. Tencent Cloud telah diakui selama empat tahun berturut-turut oleh lembaga penelitian industri terkemuka internasional Gartner, menempati posisi kedua di antara vendor China dalam dimensi kuadran strategis. Kesesuaian dengan Budaya

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21		berwenang untuk melakukan pemeriksaan dalam rangka memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan; 4. menyatakan tidak berkeberatan dalam hal Otoritas Jasa Keuangan dan/atau pihak lain yang sesuai undang-undang berwenang untuk melakukan pemeriksaan, akan melakukan pemeriksaan terhadap kegiatan penyediaan jasa yang diberikan; 5. sebagai pihak terafiliasi, menjaga keamanan seluruh informasi termasuk rahasia Bank dan data pribadi nasabah; 6. hanya dapat melakukan pengalihan sebagian kegiatan (subkontrak) berdasarkan persetujuan Bank yang dibuktikan dengan dokumen	Perusahaan dan Strategi Pengembangan Masa Depan Organisasi: Tencent Cloud dapat menyesuaikan solusi sesuai kebutuhan pelanggan, sehingga fleksibel beradaptasi dengan budaya dan strategi perusahaan yang berbeda. • Tingkat Keakraban dengan Industri Perbankan: Tencent Cloud telah menyediakan berbagai solusi yang disesuaikan bagi sejumlah lembaga keuangan, menawarkan solusi layanan sistematis "platform teknologi + ahli keamanan" untuk perusahaan finansial, sehingga secara efektif mengatasi tantangan keamanan, meningkatkan kemampuan perlindungan keamanan, dan memenuhi persyaratan kepatuhan keamanan. • Kemampuan Mengikuti Langkah Inovasi Pasar: Tencent Cloud secara aktif mengikuti tren pasar dan perkembangan teknologi, terus meluncurkan produk dan layanan inovatif guna mempertahankan posisi terdepannya di pasar serta memenuhi kebutuhan terbaru pelanggan. Dalam hal menandatangani perjanjian kontrak dengan pelanggan, Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			tertulis;	internasionalnya seperti KETENTUAN LAYANAN , General Service Level Agreement , Perjanjian Privasi dan Keamanan Data , yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut.
			7. melaporkan kepada Bank setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Bank;	layanan cloud yang disediakan Tencent Cloud untuk pelanggan disampaikan berdasarkan Service Level Agreement (SLA) yang disepakati untuk setiap layanan. Indikator kinerja, standar pengukuran, serta persyaratan pelaporan untuk setiap layanan dijelaskan secara jelas dalam SLA setiap produk dan dipublikasikan di situs web resmi Tencent Cloud. Tencent Cloud secara berkelanjutan melacak kinerja dan ketersediaan layanan cloud, serta menyediakan pemantauan real time bagi pelanggan melalui konsol manajemen.
			8. menyampaikan hasil audit Teknologi Informasi yang dilakukan auditor independen secara berkala terhadap penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi, kepada Otoritas Jasa Keuangan melalui Bank yang bersangkutan;	Untuk skenario penanganan subkontrak , perjanjian juga mencakup klausul seperti persetujuan sebelumnya untuk subkontrak, pemberitahuan sebelum
			9. menyediakan Rencana Pemulihan Bencana yang teruji dan memadai;	
			10. bersedia untuk kemungkinan penghentian perjanjian sebelum jangka waktu perjanjian berakhir	

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		(early termination); dan 11. memenuhi tingkat layanan sesuai dengan service level agreement antara Bank dan pihak penyedia jasa Teknologi Informasi. (4) Penggunaan pihak penyedia jasa Teknologi Informasi oleh Bank sebagaimana dimaksud pada ayat (3) wajib didasarkan pada perjanjian tertulis yang paling sedikit memuat kesediaan pihak penyedia jasa Teknologi Informasi untuk menyelenggarakan dan/atau melakukan hal-hal sebagaimana dimaksud pada ayat (3) huruf i.	penambahan atau penggantian subkontrak, serta kewajiban perlindungan data. Tanpa persetujuan sebelumnya dari pelanggan, Tencent Cloud tidak akan mensubkontrakkan operasi pemrosesan apa pun yang dilaksanakan atas nama pelanggan berdasarkan kontrak/perjanjian. Setiap perubahan yang diantisipasi terkait penambahan atau penggantian pihak subkontrak pemrosesan akan diberitahukan kepada pelanggan melalui saluran seperti email. Untuk pemantauan dan evaluasi berkelanjutan pelanggan terhadap Tencent Cloud, Tencent Cloud akan bekerja sama dengan audit keamanan dan pengawasan pihak ketiga yang dilakukan pelanggan berdasarkan situasi aktual serta kesepakatan dan perjanjian dengan pelanggan. Tencent Cloud akan menyediakan personel khusus untuk memberikan bantuan, serta merespons dan mendukung secara aktif setiap aktivitas audit yang dimulai oleh pelanggan. Tim keamanan Tencent Cloud secara berkelanjutan melakukan pemantauan dan penilaian terhadap risiko keamanan internal untuk memastikan efektivitas dan keandalan sistem manajemen keamanan informasi. Selain itu, tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			sekali setahun dan terus memantau kondisi platform cloud serta sistem internal untuk memastikan postur keamanan yang baik, sesuai dengan ketentuan dan persyaratan peraturan perundang-undangan serta standar manajemen keamanan yang berlaku. Tencent Cloud juga menjalani audit profesional oleh pihak ketiga independen setiap tahun. Melalui laporan Sistem dan Kontrol Organisasi (SOC) yang bersifat asersi, Tencent Cloud mengungkapkan kondisi terkini pengendalian internal organisasi layanannya kepada lembaga pengguna cloud, auditor independen, regulator, pemegang saham perusahaan, serta pihak-pihak terkait lainnya. Untuk memastikan kebijakan, prosedur, proses, dan langkah pengendalian teknologi informasi Tencent Cloud memenuhi persyaratan regulasi keuangan Indonesia, Tencent Cloud telah lolos audit kepatuhan IT industri keuangan Indonesia yang dilakukan oleh pihak ketiga independen dan sertifikasi SNI 27001. Pelanggan dapat mengunduh laporan terbaru secara mandiri dari Pusat Dokumen Kepatuhan Tencent Cloud. Ketika pelanggan perlu mengakhiri perjanjian kontrak karena perubahan bisnis atau perencanaan TI di masa depan, pelanggan dapat memilih untuk melakukan pencadangan dan migrasi data cloud serta lingkungan produksi kapan saja. Tencent Cloud mendukung

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
				pelanggan dalam menggunakan format standar umum untuk mencadangkan atau memigrasikan data. Dengan demikian, pelanggan dapat menggunakan metode transfer dan protokol transfer yang sama seperti pada tahap migrasi ke cloud, atau menggunakan produk layanan Direct Connect (DC) dan VPN Connection, guna memastikan keamanan dan keandalan data selama tahap migrasi keluar dari cloud. Setelah layanan cloud diakhiri, Tencent Cloud akan mengikuti metode penghapusan data yang ketat dan menghapus sepenuhnya data pelanggan, termasuk salinan dan cadangannya, setelah periode retensi berakhir. Data yang telah dihapus tidak dapat dipulihkan. Ketika media yang digunakan untuk menyediakan layanan Tencent Cloud mengalami kerusakan dan perlu diganti atau telah mencapai akhir masa pakai sehingga harus dibuang, Tencent Cloud juga akan segera melakukan penghancuran fisik secara menyeluruh sesuai dengan prosedur yang ketat. Jika pelanggan perlu memberikan akses ke sistem elektronik atau data elektronik kepada regulator, pelanggan dapat menggunakan Cloud Object Storage (COS) yang

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			disediakan oleh Tencent Cloud. Layanan ini merupakan penyimpanan terdistribusi untuk file berskala besar, memungkinkan pengguna menyimpan dan melihat data kapan saja melalui jaringan. Pengguna dapat mengelola hak akses ke bucket dan objek. Ketika menerima permintaan untuk suatu sumber daya, COS akan memeriksa Access Control List (ACL) yang relevan untuk memverifikasi apakah peminta memiliki hak akses yang diperlukan. Setelah akun sub-Tencent Cloud dibuat, pengguna dapat memberikan otorisasi kepada akun sub melalui kebijakan akses; jika perlu membuka sumber daya kepada pengguna non-Tencent Cloud, hal ini dapat dilakukan dengan mengatur izin publik (baca publik) pada sumber daya (bucket, objek, direktori). Melalui fungsi-fungsi di atas, pelanggan dapat memberikan data elektronik kepada regulator sesuai persyaratan untuk diakses. Selain itu, Tencent Cloud berkomitmen untuk melindungi keamanan data pelanggan global dan mematuhi hukum dan peraturan yang berlaku di negara atau wilayah tempat bisnis beroperasi. Pelanggan memiliki kepemilikan dan kendali tunggal atas konten data mereka sendiri. Data pelanggan di dalam Tencent Cloud dikategorikan sebagai data dengan tingkat keamanan tinggi. Kecuali untuk keperluan penyediaan layanan atau pemecahan masalah, dan setelah mendapatkan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			otorisasi eksplisit dari pelanggan, atau dalam situasi seperti investigasi peristiwa kriminal oleh otoritas pemerintah nasional atau lokal yang sesuai dengan peraturan perundang-undangan, karyawan internal Tencent Cloud tidak akan secara aktif mengakses data pelanggan mana pun.
N/A	9.3.4	Pengendalian Risiko Lainnya	Meskipun Bank maupun pihak penyedia jasa TI sudah menggunakan sistem yang canggih namun masih memungkinkan adanya penyimpangan misalnya kesalahan manusia, penerapan prosedur yang lemah dan pencurian oleh pegawai. Bank harus memastikan adanya pengendalian pengamanan untuk memitigasi risiko dan mencakup hal-hal: a. pihak penyedia jasa TI harus melakukan penelitian latar belakang para pegawainya; b. memastikan kewajiban pihak penyedia jasa TI	Pelanggan harus meminta penyedia layanan TI untuk melakukan pemeriksaan latar belakang terhadap karyawan mereka, serta dengan jelas menetapkan kewajiban dan tanggung jawab keamanan informasi serta keamanan data penyedia TI dalam perjanjian, guna memastikan bahwa biaya keamanan sesuai dengan tingkat keamanan yang diperlukan. Tencent Cloud menandatangani perjanjian kerahasiaan dengan karyawan internal, yang mencakup kewajiban dan tanggung jawab kerahasiaan penandatanganan, serta sanksi yang mungkin diterima jika melanggar klausul kerahasiaan. Karyawan outsourcing juga harus menjalani pemeriksaan latar belakang sebelum dipekerjakan dan tunduk pada persyaratan kerahasiaan yang ditetapkan dalam perjanjian antara Tencent Cloud dan penyedia outsourcing. Persyaratan kerahasiaan antara Tencent Cloud dengan karyawan dan pihak ketiga ditinjau dan diperbarui oleh departemen hukum sesuai kebutuhan. Dalam hal kontrak dan perjanjian,

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		melakukan pengendalian keamanan terhadap seluruh fasilitas TI yang digunakan dan data yang diproses serta informasi yang dihasilkan telah dicantumkan dalam perjanjian; c. memastikan pihak penyedia jasa TI memahami dan dapat memenuhi tingkat pengamanan yang dibutuhkan Bank untuk masing-masing jenis data berdasarkan sensitivitas kerahasiaan data; d. memastikan biaya yang dikeluarkan untuk masing-masing pengamanan sebanding dengan tingkat pengamanan yang dibutuhkan dan sesuai dengan tingkat toleransi risiko yang telah ditetapkan oleh Bank.	Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN, General Service Level Agreement, Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut.
N/A	9.4	Pengendalian Intern dan Audit Intern	Bank harus memiliki program pemantauan untuk memastikan penyedia jasa TI telah melaksanakan	Pelanggan harus melakukan tinjauan sebelum dan sesudah bekerja sama dengan penyedia layanan TI, serta melakukan peninjauan berkala terhadap kinerja dan pencapaian SLA.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			pekerjaan atau memberikan jasa sesuai dengan perjanjian. Sumber daya untuk mendukung program ini dapat bervariasi tergantung pada kritikalitas dan kompleksitas sistem, proses, dan jasa yang dikerjakan penyedia jasa TI.	Untuk mendukung persyaratan pengawasan outsourcing pelanggan, Tencent Cloud akan bekerja sama dengan audit keamanan dan pengawasan pihak ketiga yang dilakukan pelanggan berdasarkan situasi aktual serta kesepakatan dan perjanjian dengan pelanggan. Tencent Cloud akan menyediakan personel khusus untuk memberikan bantuan, serta merespons dan mendukung secara aktif setiap aktivitas audit yang dimulai oleh pelanggan.
			Bank harus melakukan kaji ulang sebelum dan setelah pekerjaan penyedia jasa TI untuk memastikan bahwa kebijakan, standar, dan prosedur manajemen risiko Bank telah dilakukan secara efektif. Selanjutnya, performance review dan pencapaian SLA dilakukan secara berkala yang didokumentasikan dalam bentuk laporan. Pemantauan harus dilakukan terhadap laporan hasil pemeriksaan penyedia jasa TI. Bank melaksanakan fungsi audit	Selain itu, tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun dan terus memantau kondisi platform cloud serta sistem internal untuk memastikan postur keamanan yang baik, sesuai dengan ketentuan dan persyaratan peraturan perundang-undangan serta standar manajemen keamanan yang berlaku. Tencent Cloud juga menjalani audit profesional oleh pihak ketiga independen setiap tahun. Melalui laporan Sistem dan Kontrol Organisasi (SOC) yang bersifat asersi, Tencent Cloud mengungkapkan kondisi terkini pengendalian internal organisasi layanannya kepada lembaga pengguna cloud, auditor independen, regulator, pemegang saham perusahaan, serta pihak-pihak terkait lainnya. layanan cloud yang disediakan Tencent Cloud untuk pelanggan disampaikan berdasarkan Service

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21		terhadap pihak penyedia jasa TI secara berkala, baik dilakukan oleh audit intern Bank maupun pihak audit ekstern yang ditunjuk oleh Bank. Ruang lingkup audit sesuai dengan cakupan jasa sebagaimana yang tertuang dalam perjanjian.	Level Agreement (SLA) yang disepakati untuk setiap layanan. Indikator kinerja, standar pengukuran, serta persyaratan pelaporan untuk setiap layanan dijelaskan secara jelas dalam SLA setiap produk dan dipublikasikan di situs web resmi Tencent Cloud. Tencent Cloud secara berkelanjutan melacak kinerja dan ketersediaan layanan cloud, serta menyediakan pemantauan real time bagi pelanggan melalui konsol manajemen.

5.9 Pelaporan

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			
31	N/A	Laporan Insidentil	(1) Bank wajib melaporkan kejadian kritis, penyalahgunaan, dan/atau kejahatan dalam penyelenggaraan Teknologi Informasi yang dapat dan/atau telah mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional Bank. (2) Laporan	Pelanggan harus segera melaporkan peristiwa besar, penyalahgunaan, atau tindak pidana dalam operasi teknologi informasi kepada Otoritas Jasa Keuangan melalui email atau telepon, dan mengajukan laporan tertulis selambat-lambatnya dalam 7 hari kerja. Dalam hal komunikasi dan pemberitahuan insiden , Tencent Cloud telah menetapkan standar manajemen insiden keamanan informasi dan membangun prosedur terkait seperti respons insiden keamanan informasi, eskalasi insiden, serta pemberitahuan insiden. Hal ini

Nomor		Domain	Ringkasan	Respons Tencent Cloud
NOMOR	NOMOR	Kontrol	Persyaratan Kontrol	
38	21			
			sebagaimana dimaksud pada ayat (1) wajib disampaikan dengan segera kepada Otoritas Jasa Keuangan melalui surat elektronik (electronic mail) atau telepon yang diikuti dengan laporan tertulis paling lama 7 (tujuh) hari kerja setelah kejadian kritis dan/atau penyalahgunaan atau kejahatan diketahui.	bertujuan untuk memberikan peringatan atau pemberitahuan tepat waktu kepada pihak internal perusahaan, pelanggan, dan pemangku kepentingan lainnya yang mungkin atau telah terkena dampak insiden, sehingga memastikan semua pihak dapat berkomunikasi dan berkoordinasi secara tertib, cepat, dan efisien. Untuk insiden keamanan yang berpotensi memengaruhi pelanggan, Tencent Cloud akan menilai cakupan dan tingkat dampak insiden keamanan informasi, kemudian setelah melalui tinjauan internal, hasil penanganan dan analisis insiden tersebut akan disampaikan kepada pelanggan melalui saluran yang sesuai. Dukungan teknis juga akan disediakan untuk membantu pelanggan mengambil langkah perbaikan guna meminimalkan kerugian. Dalam hal pelanggan melaporkan masalah atau menghubungi Tencent Cloud secara aktif, konsol resmi Tencent Cloud menyediakan layanan tiket yang mendukung pelanggan untuk melaporkan gangguan, insiden, masalah, dan keluhan terkait keamanan, ketersediaan, dan kerahasiaan. Tencent Cloud menyediakan layanan pelanggan online dan saluran telepon melalui konsol cloud serta

Nomor		Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
NOMOR	NOMOR			
38	21			situs web resminya untuk mendukung pelanggan dalam memberikan umpan balik terkait masalah yang dihadapi saat menggunakan layanan Tencent Cloud. Tencent Cloud memiliki pusat layanan pelanggan dengan cadangan lintas wilayah yang mampu menangani permintaan pelanggan secara non-stop 7*24 jam, menyediakan dukungan teknis sepanjang waktu untuk produk cloud, serta respons dan penanganan layanan yang tepat waktu dan berkualitas tinggi. Pelanggan juga dapat memilih paket layanan yang sesuai untuk mendapatkan dukungan eksklusif yang terdiri dari grup dukungan khusus, manajer layanan teknis khusus, layanan bernilai tambah, dan komponen lainnya.

06

Bagaimana Tencent Cloud Mematuhi dan Membantu Pelanggan Memenuhi Peraturan Penerapan Teknologi Informasi untuk Bank Umum dan Lembaga Jasa Keuangan Non-Bank

Penerapan teknologi informasi meningkatkan eksposur risiko yang dihadapi oleh lembaga keuangan. Lembaga keuangan perlu memperkuat tata kelola teknologi informasi dan mengoptimalkan sumber daya untuk mengurangi tekanan risiko, sehingga menciptakan nilai tambah bagi bisnis. Oleh karena itu, Otoritas Jasa Keuangan Indonesia menetapkan dan menerbitkan [NOMOR 4 /POJK.05/2021 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Lembaga Jasa Keuangan Nonbank](#) guna mengatur dan menyempurnakan manajemen risiko dalam proses penggunaan teknologi informasi oleh Lembaga Jasa Keuangan Non-Bank (LJKNB)¹.

Selain itu, untuk menyelaraskan secara dinamis penerapan dan standar perkembangan teknologi informasi, Otoritas Jasa Keuangan Indonesia merevisi lebih lanjut NOMOR 38 /POJK.03/2016 beserta perubahannya, dan menerbitkan [NOMOR 11 /POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi](#) pada tahun 2022.

Kedua peraturan tersebut menekankan persyaratan klausul terutama pada tata kelola teknologi informasi, struktur organisasi teknologi informasi, penerapan manajemen risiko operasional teknologi informasi, penggunaan penyedia layanan teknologi informasi, penyebaran sistem elektronik, perlindungan data pribadi, dan aspek-aspek lainnya, dengan konten klausul yang sangat mirip. Oleh karena itu, dalam bab ini, Tencent Cloud akan merangkum dan mengintegrasikan persyaratan kontrol yang terkait dengan penyedia layanan cloud dari NOMOR 4 /POJK.05/2021 dan NOMOR 11 /POJK.03/2022.

Selanjutnya, akan dijelaskan bagaimana Tencent Cloud, sebagai penyedia layanan cloud, dapat membantu bank umum dan lembaga jasa keuangan non-bank mematuhi persyaratan terkait.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
9	N/A	kecukupan kebijakan	(1) LJKNB wajib memiliki kebijakan	Pelanggan harus menetapkan kebijakan, standar, dan prosedur

¹ Lembaga Jasa Keuangan Nonbank yang selanjutnya disebut LJKNB adalah lembaga yang melaksanakan kegiatan di sektor perasuransian, dana pensiun, lembaga pembiayaan, dan lembaga jasa keuangan lainnya.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
		dan prosedur penggunaan teknologi informasi	dan prosedur penggunaan Teknologi Informasi. (2) LJKNB wajib menerapkan kebijakan dan prosedur penggunaan Teknologi Informasi. (3) Kebijakan dan prosedur penggunaan Teknologi Informasi memuat aspek paling sedikit: a. manajemen; b. pengembangan dan pengadaan; c. operasional Teknologi Informasi; d. jaringan komunikasi; e. pengamanan informasi; f. Rencana Pemulihan Bencana; g. penggunaan pihak penyedia jasa Teknologi Informasi; h. Layanan Keuangan Elektronik, bagi LJKNB yang menyelenggarakan Layanan Keuangan Elektronik. (4) LJKNB wajib menetapkan limit risiko yang dapat ditoleransi untuk memastikan aspek terkait Teknologi Informasi sebagaimana	penggunaan teknologi informasi, serta secara berkala meninjau dan memperbarui kebijakan dan prosedur tersebut. Pelanggan juga perlu menetapkan toleransi tingkat risiko untuk memastikan aspek-aspek terkait teknologi informasi dapat beroperasi secara optimal. Guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Tim keamanan Tencent Cloud secara berkelanjutan memantau dan mengevaluasi risiko keamanan internal untuk menjaga efektivitas dan keandalan sistem manajemen keamanan informasi. Tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun, dan secara terus-menerus

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			dimaksud pada ayat (3) dapat berjalan dengan optimal. (5) LJKNB wajib melakukan kaji ulang dan pengkinian atas kebijakan dan prosedur sebagaimana dimaksud pada ayat (2) secara berkala. (6) LJKNB wajib menetapkan jangka waktu kaji ulang dan pengkinian atas kebijakan dan prosedur sebagaimana dimaksud pada ayat (5) dalam kebijakan secara tertulis.	memantau kondisi platform cloud dan sistem internal, memastikan bahwa mereka mempertahankan postur keamanan yang baik dan mematuhi peraturan dan persyaratan standar manajemen keamanan serta peraturan perundang-undangan yang berlaku.
11	15	manajemen risiko	(1) Bank dan LJKNB wajib menerapkan manajemen risiko secara efektif dalam penyelenggaraan TI. (2) Penerapan manajemen risiko sebagaimana dimaksud pada ayat (1) harus dilakukan secara terintegrasi dalam setiap tahapan penyelenggaraan TI. (3) Dalam menerapkan manajemen risiko sebagaimana dimaksud pada ayat	Pelanggan harus secara berkala melakukan penilaian risiko teknologi informasi, mengumpulkan aktivitas teknologi informasi yang berpotensi menimbulkan atau meningkatkan risiko, menganalisis secara kualitatif dan kuantitatif risiko yang telah diidentifikasi berdasarkan tingkat dampak dan frekuensi terjadinya, menetapkan prioritas tindakan pengendalian, serta menerapkan langkah-langkah mitigasi risiko. Pelanggan juga perlu terus memantau dan melacak pelaksanaan kegiatan pengendalian dan mitigasi terhadap risiko yang telah diidentifikasi. Dalam rangka mendukung kepatuhan pelanggan terhadap persyaratan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			(1), Bank dan LJKNB melakukan proses paling sedikit:	regulasi, Tencent Cloud secara internal menetapkan prosedur manajemen risiko keamanan informasi, yang secara jelas mendefinisikan dan memberikan panduan untuk seluruh proses manajemen risiko (identifikasi risiko, analisis risiko, penyusunan rencana penanganan risiko, serta pelacakan dan pemantauan risiko).
			a. identifikasi risiko;	
			b. pengukuran risiko;	
			c. pemantauan risiko; dan	
			d. pengendalian risiko.	
			(4) Bank dan LJKNB wajib memastikan kecukupan sistem informasi manajemen risiko dalam penyelenggaraan TI.	• Identifikasi Risiko: Tencent Cloud secara berkala melaksanakan penilaian risiko, mengidentifikasi skenario risiko yang relevan berdasarkan laporan insiden keamanan industri, pengalaman praktis Tencent Cloud, serta basis data risiko dari lembaga profesional. Identifikasi risiko dilakukan melalui analisis terhadap skenario risiko serta hasil analisis proses bisnis, produk, atau layanan. • Penilaian Risiko: Tencent Cloud mengevaluasi nilai aset, kemungkinan terjadinya risiko dalam skenario tertentu, serta tingkat dampak risiko, kemudian menghitung tingkat risiko berdasarkan parameter tersebut. • Penanganan Risiko: Berdasarkan hasil analisis risiko, Tencent Cloud menerapkan strategi respons dan langkah-langkah mitigasi yang sesuai untuk setiap risiko yang teridentifikasi. Untuk risiko tinggi, penanggung jawab risiko

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				menyusun rencana penanganan (melalui transfer risiko atau tindakan pengurangan risiko) dan memperbarui tabel manajemen risiko. Untuk risiko sedang, penanggung jawab risiko menilai kebutuhan penyusunan rencana penanganan berdasarkan kondisi aktual. Untuk risiko rendah, risiko tersebut dianggap dapat diterima. Tencent Cloud juga secara berkala meninjau risiko residua untuk memantau status dan nilai risikonya. • Pemantauan, Tinjauan, dan Pelaporan Risiko: Tencent Cloud mengumpulkan hasil penilaian risiko, menghasilkan laporan penilaian risiko, dan menyampaikannya kepada manajemen. Selain itu, Tencent Cloud memelihara tabel manajemen risiko, memantau perubahan kondisi risiko serta status rencana penanganan risiko, dan menyesuaikan rencana manajemen risiko secara real time. Selain itu, Tencent Cloud mendefinisikan indikator risiko kunci dan secara berkala melakukan pengukuran terhadap indikator tersebut. Dengan membandingkannya terhadap kriteria risiko yang dapat diterima, Tencent Cloud menganalisis akar penyebab masalah yang ditemukan serta mengusulkan rekomendasi dan solusi perbaikan.
12	N/A	Pengemban	(1) Dalam melakukan	Pelanggan harus menetapkan dan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
		gan Teknologi Informasi	pengembangan Teknologi Informasi, LJKNB wajib melakukan langkah pengendalian untuk menghasilkan sistem yang mendukung: a. pencapaian tujuan LJKNB; dan b. terjaganya kerahasiaan dan integrasi data. (2) Langkah pengendalian sebagaimana dimaksud pada ayat (1) mencakup paling sedikit: a. menetapkan dan menerapkan metodologi dan prosedur pengembangan dan pengadaan Teknologi Informasi secara konsisten; b. menerapkan manajemen proyek dalam pengembangan dan pengadaan sistem; c. melakukan uji coba secara memadai dalam pengembangan dan pengadaan suatu sistem, termasuk uji coba bersama satuan kerja pengguna,	melaksanakan proses serta rencana pengembangan dan pengadaan teknologi informasi, menerapkan manajemen proyek, melakukan pengujian yang memadai, serta mendokumentasikan seluruh proses saat melakukan pengembangan dan pengadaan teknologi informasi. Selain itu, pelanggan perlu membangun mekanisme manajemen perubahan sistem aplikasi untuk memastikan bahwa sistem teknologi informasi dapat dilacak secara lengkap. Jika perangkat lunak yang digunakan pelanggan dikembangkan oleh pihak ketiga dan tidak menyediakan kode sumber, pelanggan harus mengevaluasi kebutuhan untuk menandatangani perjanjian escrow tertulis dengan pihak ketiga tersebut. Untuk mendukung pelanggan dalam manajemen pengembangan, Tencent Cloud menyediakan alat pengembang Cloud Native Build (CNB). CNB berbasis ekosistem Docker, yang mengabstraksikan lingkungan, cache, dan plugin, serta menggunakan sintaks deklaratif, bertujuan membantu pengembang membangun perangkat lunak dengan cara yang lebih efisien. CNB menyediakan rangkaian lengkap alat pengembang, dengan kemampuan seperti hosting kode, pipeline pengembangan berkinerja tinggi, peninjauan kode AI, lingkungan pengembangan berbasis cloud, manajemen artefak, dan kumpulan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			untuk memastikan keakuratan dan berfungsinya sistem sesuai kebutuhan pengguna serta kesesuaian sistem yang satu dengan sistem yang lain; d. melakukan dokumentasi atas pengembangan, pengadaan, dan pemeliharaan sistem Teknologi Informasi; e. memiliki manajemen perubahan sistem Teknologi Informasi; f. memastikan sistem Teknologi Informasi LJKNB mampu menampilkan kembali informasi secara utuh; g. memastikan pembuatan perjanjian tertulis atas perangkat lunak dalam hal perangkat lunak memengaruhi kelangsungan operasional LJKNB dan dibuat oleh pihak lain.	tugas yang dapat disesuaikan, yang secara efektif dapat mendukung seluruh alur proses pengembangan dari kebutuhan hingga penyebaran serta manajemen pengembangan yang gesit. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN、General Service Level Agreement、Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. Untuk mendukung pelanggan dalam memenuhi persyaratan regulasi, dalam hal pengembangan keamanan sistem, Tencent Cloud telah membangun seperangkat standar pengembangan keamanan sistem informasi internal. Tencent Cloud berupaya mengintegrasikan standar ISO/IEC 20000 (Manajemen Layanan Teknologi Informasi), ISO/IEC 27001 (Sistem Manajemen Keamanan Informasi), dan ISO/IEC 9001 (Sistem Manajemen Mutu) ke dalam seluruh siklus hidup pengembangan keamanan produk. Hal ini dilakukan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				dengan memperhatikan berbagai tahapan seperti analisis kebutuhan, desain, pengembangan, pengujian, penerapan, dan pemeliharaan, untuk menghilangkan masalah keamanan informasi dan privasi pada setiap tahap pengembangan produk, serta memastikan bahwa produk cloud mendapatkan pengendalian keamanan yang memadai selama siklus hidupnya. Tindakan pengendalian keamanan terkait meliputi: • Pelatihan Keamanan: Meningkatkan kesadaran pemrograman aman di kalangan pengembang, dan secara ketat mewajibkan personel terkait untuk mematuhi standar pengkodean yang aman. • Analisis Kebutuhan: Berkomunikasi mengenai konten bisnis, alur proses bisnis, dan kerangka teknologi untuk menemukan cara optimal dalam mengintegrasikan keamanan. • Desain Sistem: Melakukan pemodelan ancaman terhadap desain sistem, serta menilai keamanan teknologi dari arsitektur yang digunakan. • Pengembangan Sistem: Selama proses pengembangan, menyediakan komponen pengembangan aman yang dirancang sendiri oleh Tencent

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				untuk digunakan oleh tim pengembang, dan melakukan pengkodean sesuai dengan standar pengkodean aman Tencent Cloud. • Verifikasi Keamanan: Mendeteksi kerentanan melalui pemeriksaan keamanan kode, pemindaian keamanan aset, pemindaian web, penilaian keamanan manual, pengujian penetrasi, dan audit kode. • Rilis: Sistem hanya dapat dirilis ke lingkungan produksi setelah semua risiko tinggi diperbaiki, guna mencegah produk dijalankan di lingkungan produksi dengan membawa kerentanan keamanan. Dalam hal pengujian sistem, setelah tim pengembangan Tencent Cloud menyelesaikan pengembangan produk baru atau ketika produk mengalami perubahan signifikan, personel pengujian menyusun rencana pengujian dan kasus uji yang sesuai berdasarkan kebutuhan produk, serta mengorganisir tim proyek untuk meninjau kasus uji tersebut. Setelah kasus uji dikonfirmasi, tim pengujian melakukan pengujian fungsional pada produk proyek untuk memastikan fungsionalitas produk tersedia, andal, dan memenuhi persyaratan kualitas produk yang ditetapkan secara internal oleh Tencent Cloud. Setelah pengujian fungsional selesai, tim keamanan

Nomor LJKNB	Domain Bank	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
				melakukan pengujian keamanan pada produk. Cacat atau kerentanan yang ditemukan selama proses pengujian ditangani sesuai dengan alur manajemen kerentanan internal Tencent Cloud. Personel penguji menghasilkan laporan pengujian berdasarkan hasil pengujian dan menyerahkannya kepada berbagai tim terkait untuk konfirmasi. Terhadap penggunaan produk pihak ketiga, Tencent Cloud menetapkan persyaratan manajemen keamanan rantai pasok perangkat lunak, dengan jelas menetapkan tinjauan keamanan saat masuknya komponen eksternal, serta melakukan penguatan dan pertahanan keamanan sebelum peluncuran, untuk memastikan produk lulus pemeriksaan keamanan pra-peluncuran. Setelah diluncurkan, produk akan menjalani operasi dan pemeriksaan keamanan berkelanjutan, menangani masalah keamanan secara tepat waktu, serta melalui evaluasi kondisi operasi keamanan produk untuk mengidentifikasi risiko keamanan, mendorong pemasok untuk melakukan perbaikan, dan meninjau strategi kerja sama selanjutnya dengan pemasok tersebut. Dalam hal manajemen perubahan, Tencent Cloud telah menetapkan seperangkat standar manajemen untuk perubahan produk dan konfigurasi. Semua jenis perubahan program, termasuk perubahan pada

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				aplikasi dan file konfigurasi, sistem operasi, serta basis data, harus melalui analisis dampak bisnis sebelum diluncurkan, menyusun rencana rollback untuk perubahan tersebut, dan mendapatkan persetujuan dari penanggung jawab terkait. Sistem rilis perubahan Tencent Cloud mewajibkan bahwa operasi perubahan hanya dapat dilakukan oleh personel yang berwenang, serta menyimpan log terkait perubahan dan melakukan audit log secara berkala. Setelah perubahan dirilis, Tencent Cloud akan memvalidasi, memantau, dan mencatat hasil perubahan di lingkungan produksi.
17	16	Pengamanan Informasi	(1) Bank dan LJKNB wajib memastikan pengamanan informasi dilaksanakan secara efektif dan efisien. (2) Pengamanan informasi sebagaimana dimaksud pada ayat (1) dilakukan terhadap aspek sumber daya manusia, proses, teknologi, dan fisik atau lingkungan, dalam penyelenggaraan TI secara menyeluruh. (3) Penerapan pengamanan informasi sebagaimana	Pelanggan harus menerapkan manajemen keamanan informasi berdasarkan hasil penilaian risiko aset informasi, mencakup aspek teknologi, sumber daya manusia, dan proses dalam penggunaan teknologi informasi, guna menjaga kerahasiaan, integritas, dan ketersediaan informasi. Guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			dimaksud pada ayat (1) dilakukan berdasarkan hasil penilaian terhadap risiko pada informasi yang dimiliki Bank dan LJKNB.	bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Tim keamanan Tencent Cloud secara berkelanjutan memantau dan mengevaluasi risiko keamanan internal untuk menjaga efektivitas dan keandalan sistem manajemen keamanan informasi. Tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun, dan secara terus-menerus memantau kondisi platform cloud dan sistem internal, memastikan bahwa mereka mempertahankan postur keamanan yang baik dan mematuhi peraturan dan persyaratan standar manajemen keamanan serta peraturan perundang-undangan yang berlaku. Tencent Cloud secara internal juga telah membangun mekanisme pelatihan keamanan informasi, yang menyediakan berbagai kursus pelatihan bagi karyawan. Materi pelatihan mencakup aspek-aspek seperti kesadaran keamanan dasar, keamanan kantor, identifikasi dan pertahanan kerentanan, perlindungan privasi, tanggap darurat, standar keamanan pengembangan, serta persyaratan keamanan data. Informasi lebih lanjut terkait aspek sumber daya manusia, proses,

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				teknologi, serta lingkungan fisik atau lingkungan, dapat dirujuk pada bagian " 5.5 Pengamanan Informasi " dalam panduan ini.
14	17	Jaringan Komunikasi	Bank dan LJKNB wajib memastikan jaringan komunikasi yang disediakan oleh Bank telah memenuhi prinsip kerahasiaan, integritas, dan ketersediaan.	Pelanggan harus menyediakan jaringan komunikasi yang memenuhi prinsip kerahasiaan, integritas, dan ketersediaan. Jaringan dasar Tencent Cloud mengadopsi metode konstruksi redundansi, yang dikombinasikan dengan teknik rekayasa lalu lintas berbasis prioritas jalur dan keterjangkauan rute pada lapisan perutean, guna memastikan bahwa layanan jaringan tidak akan terputus akibat kegagalan perangkat tunggal. Node komputasi Tencent Cloud juga dibangun dengan skema redundansi. Ketika terjadi kegagalan pada satu node komputasi, penjadwal (scheduler) akan secara otomatis dan real time mengecualikan node tersebut, sehingga secara efektif menjaga ketersediaan layanan pelanggan. Dalam hal keamanan komunikasi jaringan, komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Antarmuka API cloud yang disediakan oleh produk-produk cloud Tencent Cloud juga dilengkapi dengan kemampuan keamanan seperti enkripsi HTTPS, verifikasi tanda tangan, dan pemantauan status, memberikan jaminan keamanan komunikasi pada tingkat

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				port untuk bisnis pelanggan. Direct Connect (DC) Menyediakan koneksi jaringan pita lebar dengan keamanan tinggi dan khusus untuk pelanggan. Pelanggan memiliki jalur jaringan eksklusif tanpa risiko kebocoran data. Cloud Connect Network (CCN), Mendukung interkoneksi jaringan internal antara VPC di cloud, serta antara VPC dan pusat data lokal (IDC). Informasi lebih lanjut terkait jaringan komunikasi teknologi informasi dapat dirujuk pada bagian "5.4 Teknologi Jaringan Komunikasi" dalam panduan ini.
16	18	Rencana Pemulihan Bencana	(1) Bank dan LJKNB wajib memiliki Rencana Pemulihan Bencana. (2) Bank dan LJKNB wajib memastikan Rencana Pemulihan Bencana sebagaimana dimaksud pada ayat (1) dapat dilaksanakan, sehingga kelangsungan operasional Bank dan LJKNB tetap berjalan saat terjadi bencana dan/atau gangguan pada sarana TI yang digunakan Bank dan LJKNB.	Pelanggan harus menyusun rencana pemulihan bencana dan mengujinya setidaknya setahun sekali berdasarkan hasil analisis dampak bisnis untuk aplikasi dan infrastruktur kritis, guna memastikan rencana tersebut dapat dilaksanakan secara efektif. Pelanggan juga perlu meninjau rencana pemulihan bencana setidaknya sekali setahun. Tencent Cloud membangun atau menyewa pusat data di berbagai lokasi global sesuai dengan standar internasional terkait dan persyaratan keamanan setempat, menyediakan pilihan multi-wilayah dan multi-zona ketersediaan bagi pelanggan untuk memenuhi persyaratan ketahanan bencana bisnis dan tingkat layanan yang diharapkan. Layanan komputasi, jaringan, penyimpanan, basis data,

Nomor LJKNB	Domain Bank	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			(3) Bank dan LJKNB wajib melakukan uji coba atas Rencana Pemulihan Bencana terhadap seluruh aplikasi dan infrastruktur yang kritikal sesuai hasil analisis dampak bisnis, paling sedikit 1 (satu) kali dalam 1 (satu) tahun dengan melibatkan pengguna TI.	serta layanan kontainer dan middleware yang disediakan oleh Tencent Cloud tidak hanya menyediakan arsitektur sistem dengan ketersediaan tinggi bagi pelanggan, tetapi juga mendukung pelanggan dalam mengonfigurasi strategi pencadangan sistem dan data mereka sendiri, memenuhi berbagai kebutuhan pencadangan pelanggan.
			(4) Bank dan LJKNB wajib melakukan kaji ulang Rencana Pemulihan Bencana paling sedikit 1 (satu) kali dalam 1 (satu) tahun.	untuk memastikan ketersediaan berkelanjutan dari bisnis pelanggan, Tencent Cloud telah merancang dan menerapkan kerangka manajemen kelangsungan bisnis yang sesuai dengan lingkungan komputasi awannya sendiri, serta telah memperoleh sertifikasi internasional ISO/IEC 22301 untuk Sistem Manajemen Kelangsungan Bisnis.
			(5) Bank dan LJKNB wajib menetapkan jangka waktu uji coba sebagaimana dimaksud pada ayat (3) dan kaji ulang sebagaimana dimaksud pada ayat (4) dalam kebijakan secara tertulis.	Tencent Cloud melakukan analisis dampak bisnis terhadap produk dan layanan cloud, menetapkan target waktu pemulihan (Recovery Time Objective/RTO) dan target titik data pemulihan (Recovery Point Objective/RPO) untuk setiap bisnis, serta menyusun strategi respons dan rencana kelangsungan bisnis yang berbeda berdasarkan hasil analisis dampak bisnis. Rencana pemulihan bencana yang rinci juga telah disusun untuk produk cloud dan proses kritis. Tencent Cloud secara berkala melakukan uji latihan kelangsungan bisnis untuk produk cloud berdasarkan rencana kelangsungan bisnis, guna memastikan kelayakan rencana, prosedur, dan elemen

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				lainnya. Tencent Cloud juga meninjau rencana kelangsungan bisnis setiap tahun dan memperbarui rencana sesuai kebutuhan berdasarkan hasil tinjauan. Ketika terjadi perubahan signifikan dalam fungsi bisnis atau sumber daya kunci, Tencent Cloud akan meninjau cakupan bisnis dan fungsi kritis serta ketergantungan komponen masing-masing, serta merevisi rencana kelangsungan bisnis secara tepat waktu. Informasi lebih lanjut terkait Rencana Kelangsungan Bisnis dapat dilihat pada bagian " 5.6 Rencana Pemulihan Bencana " dalam panduan ini.
N/A	21	Ketahanan Siber	(1) Bank wajib menjaga ketahanan siber. (2) Untuk menjaga ketahanan siber sebagaimana dimaksud pada ayat (1), Bank melakukan proses paling sedikit: a. identifikasi aset, ancaman, dan kerentanan; b. perlindungan aset; c. deteksi insiden siber; dan d. penanggulangan dan pemulihan insiden siber. (3) Bank memastikan proses untuk menjaga ketahanan	Pelanggan harus membangun proses perlindungan aset, identifikasi ancaman dan kerentanan, deteksi insiden jaringan, serta respons dan pemulihan untuk memastikan ketahanan teknologi informasi terhadap risiko. Pelanggan juga dapat menggunakan platform manajemen keamanan terpadu Tencent Cloud, Cloud Security Center (CSC), untuk mengelola keamanan aset informasi. CSC mencakup fungsionalitas Asset Security Center, yang membantu pelanggan dalam melakukan inventarisasi dinamis otomatis terhadap aset di cloud, termasuk server cloud, penyimpanan objek, database cloud, penyeimbang beban, dan lainnya. Melalui berbagai dimensi keamanan seperti risiko konfigurasi

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			siber sebagaimana dimaksud pada ayat (2) didukung dengan sistem informasi ketahanan siber yang memadai.	cloud, kerentana, dan insiden keamanan, CSC menyediakan manajemen terpadu terhadap risiko keamanan aset, sehingga mengurangi risiko "IT bayangan" (shadow IT) di cloud. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar manajemen aset informasi dan proses manajemen siklus hidup lengkap. Hal ini mencakup pengelolaan dan perlindungan aset seperti data elektronik, perangkat keras dan perangkat virtualnya, infrastruktur, sistem aplikasi, serta perangkat lunak melalui klasifikasi dan penilaian tingkat kepentingan. Tencent Cloud mengelola perangkat keras dan komponen perangkat lunak menggunakan sistem manajemen aset, yang meliputi pendaftaran dan pengikatan aset, inventarisasi dan pembaruan informasi aset, serta pensiun dan penggantian aset. Tujuannya adalah untuk memastikan operasi yang stabil dari sistem dasar platform cloud dan memberikan dukungan yang andal bagi sistem bisnis. Untuk mendukung pelanggan dalam mendeteksi insiden dan merespons dengan cepat, Tencent Cloud menyediakan platform manajemen keamanan terpadu Cloud Security Center (CSC). Melalui

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				fungsionalitas seperti Pusat Aset, Pusat Risiko, Pusat Peringatan, dan Manajemen Keamanan Tingkat Lanjut, CSC membantu pelanggan mencapai siklus operasi keamanan yang mencakup deteksi ancaman sebelum insiden, respons dan penanganan selama insiden, serta analisis forensik pasca-insiden, sehingga meningkatkan efisiensi operasi keamanan. Dalam hal manajemen insiden, Tencent Cloud telah menetapkan prosedur internal untuk mengelola insiden dan permintaan layanan, serta membangun kebijakan manajemen insiden Tencent Cloud. Hal ini memastikan bahwa insiden terkait aktivitas manajemen layanan TI dicatat dan diklasifikasikan, diprioritaskan berdasarkan tingkat dampak dan urgensi, serta ditingkatkan (escalated) sesuai kebutuhan. Tujuannya adalah untuk menyelesaikan dan menutup berbagai jenis insiden dengan cepat, meminimalkan dampak insiden, menjaga kelancaran operasional bisnis, serta meningkatkan kepuasan pelanggan. Untuk mendukung pelanggan dalam mendeteksi dan menganalisis ancaman, Tencent Cloud menyediakan Threat Intelligence Center (TIX). Sebagai platform layanan intelijen terpadu,

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				TIX menyediakan tiga kemampuan intelijen utama: intelijen dasar, intelijen permukaan serangan, dan intelijen bisnis. Platform ini mendukung fungsi seperti kueri intelijen, analisis dan penilaian IOC, serta manajemen permukaan serangan. Kemampuan ini membantu pelanggan menganalisis dan menilai insiden keamanan dengan lebih efisien, serta menilai risiko paparan aset perusahaan secara lebih komprehensif, sehingga mendukung pembangunan sistem pertahanan keamanan multidimensi yang efektif. TIX membangun jaringan titik kontak intelijen yang lengkap, mengumpulkan dan menganalisis intelijen ancaman dari berbagai sumber seperti komunitas kerentanan, lembaga keamanan, penyedia alat keamanan, media sosial, dan blog keamanan. Platform ini juga terintegrasi dengan algoritma dan daya komputasi cloud untuk menghilangkan alarm palsu, sehingga memastikan keakuratan intelijen.
N/A	23	Pengujian Keamanan Siber	Bank wajib melakukan pengujian keamanan siber berdasarkan: a. analisis kerentanan; dan b. skenario.	Pelanggan harus secara berkala melaksanakan pengujian berbasis analisis kerentanan dan menyampaikan hasil pengujian tersebut kepada Otoritas Jasa Keuangan. Selain itu, pelanggan juga perlu melakukan pengujian keamanan siber dengan skenario simulasi setidaknya sekali setahun, dan menyampaikan laporan hasil pengujian keamanan siber kepada Otoritas Jasa Keuangan selambat-lambatnya sepuluh hari kerja setelah
N/A	24	Pengujian Keamanan Siber Berdasarkan Analisis Kerentana	(1) Pengujian keamanan siber berdasarkan analisis kerentanan sebagaimana dimaksud dalam Pasal	

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
N/A	25	Pengujian Keamanan Siber Berdasarkan Skenario Sebagaimana a	23 huruf a wajib dilaksanakan secara berkala. (2) Bank wajib menyampaikan hasil pengujian keamanan siber berdasarkan analisis kerentanan sebagaimana dimaksud pada ayat (1) kepada Otoritas Jasa Keuangan sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank.	pengujian selesai. Dalam hal pengujian penetrasi, Tencent Cloud menyediakan layanan Penetration Testing Service (PTS) bagi pelanggan. Layanan ini sepenuhnya mensimulasikan teknik serangan dan deteksi kerentanan yang mungkin digunakan oleh peretas, dengan menerapkan metode dan pendekatan yang terkendali serta non-destruktif untuk melakukan pemeriksaan mendalam terhadap keamanan sistem target. Hal ini membantu mengidentifikasi kelemahan dalam target dan perangkat jaringan, memberikan rekomendasi penguatan keamanan untuk meningkatkan keamanan sistem pelanggan, serta mendukung verifikasi setelah perbaikan kerentanan dilakukan. Dalam hal pemindaian kerentanan, pelanggan dapat memilih Vulnerability
			(1) Pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud dalam Pasal 23 huruf b wajib dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun. (2) Pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud pada ayat (1) paling sedikit mencakup: a. penetapan tujuan, cakupan, dan skenario pengujian; b. pelaksanaan pengujian; c. evaluasi hasil	Scanning Service (VSS) untuk mendeteksi aset jaringan perusahaan dan mengidentifikasi risikonya. Berdasarkan pengalaman keamanan dan intelijen ancaman yang dikumpulkan Tencent selama bertahun-tahun, VSS telah membangun basis aturan kerentanan yang kaya dan komprehensif, serta memiliki kemampuan deteksi kerentanan 0Day/1Day/NDay yang profesional dan efisien. Layanan ini dapat melakukan pemindaian keamanan berkala, peringatan risiko berkelanjutan, dan deteksi kerentanan terhadap ketersediaan,

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			pengujian; dan d. penilaian terhadap efektivitas upaya mitigasi, respon, dan tindakan pemulihan Bank terhadap serangan siber. (3) Bank wajib menyampaikan laporan hasil pengujian keamanan siber berdasarkan skenario sebagaimana dimaksud pada ayat (1) kepada Otoritas Jasa Keuangan paling lama 10 (sepuluh) hari kerja setelah pengujian keamanan siber selesai dilaksanakan. (4) Laporan hasil pengujian keamanan siber sebagaimana dimaksud pada ayat (3) paling sedikit mencakup: a. ringkasan pelaksanaan pengujian; b. pelajaran terpetik atau hasil observasi dari hasil pengujian; c. rencana atau perbaikan yang telah dilakukan.	keamanan, serta kepatuhan aset pelanggan, sekaligus memberikan rekomendasi perbaikan yang profesional untuk mengurangi risiko keamanan. VSS juga mendukung integrasi dengan produk cloud seperti Host Security dan Web Application Firewall, mencapai siklus tertutup dari pemantauan risiko hingga penanganan risiko. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud secara berkala menghasilkan tugas pemindaian melalui sistem pemindaian kerentanan untuk memindai aset di lingkungan cloud, serta menganalisis, mengklasifikasikan, dan menangani kerentanan yang ditemukan. Selain itu, Tencent Cloud secara berkala melaksanakan pengujian penetrasi skala besar pada seluruh rantai layanan, guna secara proaktif mengidentifikasi dan memperbaiki potensi risiko keamanan sistem sedini mungkin. Pengujian penetrasi yang ditargetkan juga dilakukan secara fleksibel dalam situasi seperti sebelum peluncuran produk baru atau perubahan besar lainnya. Hasil pengujian penetrasi dikomunikasikan ke departemen terkait melalui tiket keamanan, dan departemen tersebut segera melakukan perbaikan kerentanan atau menerapkan langkah pengendalian kompensasi lainnya, guna memastikan kerentanan yang dieksploitasi selama pengujian penetrasi telah ditangani dengan

Nomor LJKNB	Domain Bank	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
				baik. Selain itu, Tencent Cloud secara berkala menyelenggarakan simulasi latihan pertahanan "Tim Merah vs Tim Biru" untuk melawan serangan siber secara realistis. Tencent Cloud juga membangun platform umpan balik kerentanan eksternal dan meluncurkan "Program Penghargaan Kerentanan" yang mengundang pakar keamanan industri untuk membantu mengidentifikasi kerentanan dan risiko keamanan sistem dari perspektif peretas, sehingga masalah keamanan dapat diperbaiki tepat waktu dan keamanan ekosistem Tencent Cloud tetap terjaga. Secara bersamaan, Tencent Cloud telah menyusun rencana tanggap darurat keamanan siber yang mencakup berbagai skenario darurat seperti serangan siber, perangkat lunak berbahaya, keamanan data, kegagalan perangkat dan fasilitas, serta peristiwa bencana. Dengan mendasarkan pada pembangunan sistem rencana tanggap darurat yang komprehensif, didukung oleh pembentukan tim penanganan darurat, serta berfokus pada standardisasi alur penanganan darurat, kemampuan dalam pemantauan peringatan dini dan penanganan insiden semakin ditingkatkan untuk mencegah dan mengurangi dampak buruk insiden keamanan siber terhadap Tencent Cloud.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
21	30	Penggunaan Pihak Penyedia Jasa TI	(1) Bank dan dan LJKNB harus mengoperasikan teknologi informasi. (2) Penyelenggaraan Teknologi Informasi oleh Bank dan LJKNB dapat dilakukan secara sendiri dan/atau menggunakan pihak penyedia jasa Teknologi Informasi. (3) Dalam hal penyelenggaraan Teknologi Informasi Bank dan LJKNB dilakukan oleh pihak penyedia jasa Teknologi Informasi sebagaimana dimaksud pada ayat (2), Bank dan LJKNB wajib: a. bertanggung jawab atas penerapan manajemen risiko; b. memiliki satuan kerja penyelenggara Teknologi Informasi; c. melakukan pengawasan atas pelaksanaan kegiatan Bank dan LJKNB yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi; d. memilih pihak penyedia jasa	Jika operasional teknologi informasi pelanggan dilaksanakan oleh penyedia layanan teknologi informasi, pelanggan harus membangun proses penggunaan penyedia layanan TI eksternal. Proses ini mencakup penyampaian kebutuhan, pengiriman permintaan proposal kepada penyedia layanan TI, pelaksanaan due diligence, penandatanganan perjanjian kontrak dengan penyedia layanan TI, serta kesepakatan klausul khusus. Selain itu, pelanggan harus memastikan bahwa penyedia layanan TI memberikan hak akses data dan informasi ketika diperlukan dalam audit internal, eksternal, atau oleh regulator. Dalam aspek due diligence, Tencent Cloud akan menunjuk personel khusus untuk menanggapi kebutuhan pemeriksaan due diligence pelanggan serta menyediakan laporan audit dari pihak ketiga independen atau laporan kontrol sistem dan organisasi yang bersifat asersi sesuai permintaan pelanggan. Dalam hal menandatangani perjanjian kontrak dengan pelanggan, Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN, General Service Level Agreement, Perjanjian Privasi dan Keamanan Data, yang secara jelas

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			Teknologi Informasi berdasarkan analisis biaya dan manfaat dengan mengikutsertakan satuan kerja penyelenggara Teknologi Informasi; e. memantau dan mengevaluasi keandalan pihak penyedia jasa Teknologi Informasi secara berkala yang menyangkut kinerja, reputasi penyedia jasa, dan kelangsungan penyediaan layanan; f. memberikan akses kepada auditor internal, auditor eksternal, auditor internal grup Bank dan LJKNB, dan/atau Otoritas Jasa Keuangan untuk memperoleh data dan informasi setiap kali dibutuhkan; g. memberikan akses kepada Otoritas Jasa Keuangan terhadap Pangkalan Data secara tepat waktu, baik untuk data terkini maupun untuk data yang telah lalu; dan h. memastikan pihak	mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. layanan cloud yang disediakan Tencent Cloud untuk pelanggan disampaikan berdasarkan Service Level Agreement (SLA) yang disepakati untuk setiap layanan. Indikator kinerja, standar pengukuran, serta persyaratan pelaporan untuk setiap layanan dijelaskan secara jelas dalam SLA setiap produk dan dipublikasikan di situs web resmi Tencent Cloud. Tencent Cloud secara berkelanjutan melacak kinerja dan ketersediaan layanan cloud, serta menyediakan pemantauan real time bagi pelanggan melalui konsol manajemen. Untuk skenario penanganan subkontrak, perjanjian juga mencakup klausul seperti persetujuan sebelumnya untuk subkontrak, pemberitahuan sebelum penambahan atau penggantian subkontrak, serta kewajiban perlindungan data. Tanpa persetujuan sebelumnya dari pelanggan, Tencent Cloud tidak akan mensubkontrakkan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			penyedia jasa Teknologi Informasi: - memiliki tenaga ahli yang memiliki keandalan dengan didukung oleh sertifikat keahlian secara akademis dan/atau secara profesional sesuai dengan keperluan penyelenggaraan Teknologi Informasi; - menerapkan prinsip pengendalian Teknologi Informasi secara memadai yang dibuktikan dengan hasil audit yang dilakukan pihak independen; - menyediakan akses bagi: a) auditor internal Bank dan LJKNB; b) auditor eksternal; c) auditor internal grup Bank dan LJKNB; d) Otoritas Jasa Keuangan; dan/atau e) pihak lain yang sesuai dengan ketentuan dalam rangka memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan; - menyatakan tidak	operasi pemrosesan apa pun yang dilaksanakan atas nama pelanggan berdasarkan kontrak/perjanjian. Setiap perubahan yang diantisipasi terkait penambahan atau penggantian pihak subkontrak pemrosesan akan diberitahukan kepada pelanggan melalui saluran seperti email. Untuk pemantauan dan evaluasi berkelanjutan pelanggan terhadap Tencent Cloud, dalam hal audit dan tinjauan pengawasan oleh pelanggan, Tencent Cloud akan bekerja sama dengan audit keamanan dan pengawasan pihak ketiga yang dilakukan pelanggan berdasarkan situasi aktual serta kesepakatan dan perjanjian dengan pelanggan. Tencent Cloud akan menyediakan personel khusus untuk memberikan bantuan, serta merespons dan mendukung secara aktif setiap aktivitas audit yang dimulai oleh pelanggan. Ketika pelanggan perlu mengakhiri perjanjian kontrak karena perubahan bisnis atau perencanaan TI di masa depan, pelanggan dapat memilih untuk melakukan pencadangan dan migrasi data cloud serta lingkungan produksi kapan saja. Tencent Cloud mendukung pelanggan dalam menggunakan format standar umum untuk mencadangkan atau memigrasikan data. Dengan demikian, pelanggan dapat menggunakan metode transfer

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			berkeberatan dalam hal Otoritas Jasa Keuangan dan/atau pihak lain yang sesuai dengan ketentuan peraturan perundang-undangan berwenang untuk melakukan pemeriksaan, akan melakukan pemeriksaan terhadap kegiatan penyediaan jasa Teknologi Informasi yang diberikan; 5. menjaga keamanan seluruh informasi termasuk rahasia Bank dan LJKNB dan data pribadi konsumen, sebagai pihak terafiliasi; 6. hanya dapat melakukan pengalihan sebagian kegiatan (subkontrak) berdasarkan persetujuan Bank dan LJKNB yang dibuktikan dengan dokumen tertulis; 7. melaporkan kepada Bank dan LJKNB setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau	dan protokol transfer yang sama seperti pada tahap migrasi ke cloud, atau menggunakan produk layanan Direct Connect (DC) dan VPN Connection, guna memastikan keamanan dan keandalan data selama tahap migrasi keluar dari cloud. Setelah layanan cloud diakhiri, Tencent Cloud akan mengikuti metode penghapusan data yang ketat dan menghapus sepenuhnya data pelanggan, termasuk salinan dan cadangannya, setelah periode retensi berakhir. Data yang telah dihapus tidak dapat dipulihkan. Informasi lebih lanjut terkait penggunaan penyedia layanan teknologi informasi dapat dilihat pada bagian "5.8 Penggunaan Pihak Penyedia Jasa TI" dalam panduan ini.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			mengganggu kelancaran operasional Bank dan LJKNB; 8. menyediakan Rencana Pemulihan Bencana yang teruji dan memadai; 9. bersedia untuk adanya kemungkinan penghentian perjanjian sebelum jangka waktu perjanjian berakhir; 10. memenuhi tingkat layanan sesuai dengan service level agreement antara Bank dan LJKNB dan pihak penyedia jasa Teknologi Informasi. (3) Penggunaan pihak penyedia jasa Teknologi Informasi sebagaimana dimaksud pada ayat (3) oleh Bank dan LJKNB wajib didasarkan pada perjanjian tertulis yang memuat paling sedikit kesediaan pihak penyedia jasa Teknologi Informasi untuk memenuhi ketentuan sebagaimana dimaksud pada ayat (3) huruf h.	

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
22	N/A	Cadang Data	(1) LJKNB yang memiliki total aset sampai dengan Rp500.000.000.000,00 (lima ratus miliar rupiah) wajib melakukan rekam cadang data aktivitas yang diproses menggunakan Teknologi Informasi, yang dilakukan secara berkala.	Pelanggan harus secara berkala mencadangkan data aktivitas yang diproses menggunakan teknologi informasi. Untuk aset melebihi Rp500.000.000.000,00, diwajibkan memiliki pusat data dan melakukan pencadangan data secara berkala. Sementara untuk lembaga keuangan non-perbankan dengan aset melebihi Rp1.000.000.000.000,00, diwajibkan memiliki pusat data dan pusat pemulihan bencana.
			(2) LJKNB yang memiliki total aset lebih dari Rp500.000.000.000,00 (lima ratus miliar rupiah) sampai dengan Rp1.000.000.000.000,00 (satu triliun rupiah) wajib:	Tencent Cloud telah membangun atau menyewa pusat data di berbagai lokasi global sesuai dengan standar internasional terkait dan persyaratan keamanan setempat. Hal ini memberikan pelanggan pilihan multi-wilayah (multi-region) dan multi-zona ketersediaan (multi-availability zone), dengan tetap mematuhi ketat peraturan perundang-undangan di yurisdiksi operasi yang melindungi privasi pengguna dan keamanan data, serta secara aktif memantau perkembangan regulasi lokal.
			a. memiliki Pusat Data; dan b. melakukan rekam cadang data aktivitas yang diproses menggunakan Teknologi Informasi, yang dilakukan secara berkala.	Pelanggan dapat dengan fleksibel menempatkan data dan sistem mereka di wilayah atau zona ketersediaan yang berbeda sesuai dengan kebutuhan pengembangan bisnis dan persyaratan keamanan data. Saat ini, Tencent Cloud memiliki tiga pusat data di Indonesia yang menyediakan beragam layanan komputasi awan, termasuk server awan (cloud server), basis data awan (cloud database), penyimpanan awan (cloud storage), dan lainnya.
			(3) LJKNB wajib menetapkan jangka waktu rekam cadang data aktivitas yang diproses menggunakan Teknologi Informasi sebagaimana	Pelanggan di Indonesia dapat memilih untuk menyimpan dan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			dimaksud pada ayat (1) dan ayat (2) dalam kebijakan secara tertulis.	memproses data mereka secara lokal di Indonesia.
			(4) LJKNB:	Berbagai layanan penyimpanan dan basis data yang disediakan Tencent Cloud dilengkapi dengan fungsi pencadangan, memenuhi berbagai kebutuhan pencadangan pelanggan. Contohnya:
			a. yang memiliki total aset lebih dari Rp1.000.000.000.000,00 (satu triliun rupiah); dan/atau	Data yang disimpan pelanggan di Cloud Object Storage (COS)
			b. yang mayoritas penyelenggaraan usahanya dilakukan dengan menggunakan Teknologi Informasi, wajib memiliki Pusat Data dan Pusat Pemulihan Bencana.	dapat disimpan secara bersamaan di beberapa wilayah yang ditentukan melalui fitur replikasi lintas wilayah. Hal ini memastikan bahwa meskipun sebagian data hilang secara tidak terduga, data lengkap masih dapat ditemukan dan dipulihkan melalui data redundan. Fitur ini juga menghindari kerugian yang dapat terjadi ketika penyimpanan di satu zona ketersediaan terkena bencana yang tidak terhindarkan, sehingga mencapai efek pencadangan multi-redundan dan pemulihan bencana lintas lokasi. Fitur pencadangan snapshot Cloud Block Storage (CBS) data bisa dicadangkan dengan mengambil snapshot cloud disk secara tepat waktu untuk mencegah kehilangan data karena gangguan atau penghapusan yang tidak disengaja serta memastikan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				pemulihan cepat jika terjadi kegagalan bisnis. • <u>Cloud File Storage (CFS)</u> menyediakan fungsi snapshot berkala, memudahkan pelanggan dalam menetapkan strategi tugas pencadangan secara fleksibel. • <u>Cloud Native Database TDSQL-C</u>, database asli cloud Tencent, mendukung dua jenis pencadangan: pencadangan logis dan pencadangan snapshot. Melalui pencadangan data lengkap serta pencadangan binlog untuk periode tertentu, seluruh kluster TDSQL-C MySQL Edition atau tabel database tertentu dapat dipulihkan ke titik waktu mana pun. • <u>TencentDB for MySQL</u> mendukung dua metode pencadangan: pencadangan otomatis dan pencadangan manual. Layanan ini juga menyediakan fungsi pencadangan lintas wilayah untuk membantu pelanggan meningkatkan kemampuan pemulihan bencana sekaligus meningkatkan keandalan data. • <u>TencentDB for MongoDB</u> menyediakan mekanisme pencadangan data otomatis dan pemulihan tanpa kehilangan data (lossless recovery), mendukung pencadangan data multi-node. Pelanggan dapat menyimpan data cadangan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				selama beberapa hari melalui mekanisme pencadangan, sehingga memudahkan pemulihan data dalam situasi bencana. Untuk data pelanggan yang disimpan di cloud, Tencent Cloud menggunakan metode seperti cadangan panas real time, penyimpanan redundan, dan pencadangan lintas wilayah untuk memastikan keamanan, keandalan, dan ketersediaan berkelanjutan dari data bisnis pelanggan yang disimpan di cloud. Tencent Cloud juga menerapkan berbagai langkah perlindungan seperti keamanan fisik, kontrol akses, dan isolasi logis, serta mendukung pelanggan dalam menggunakan Key Management Service (KMS) dan Cloud Access Management (CAM) untuk mencegah akses atau perubahan tidak sah terhadap data cadangan pelanggan.
23	35	Penempatan Sistem Elektronik	(1) Bank wajib menempatkan Sistem Elektronik pada Pusat Data dan Pusat Pemulihan Bencana di wilayah Indonesia. LJKNB yang memiliki Pusat Data dan/atau Pusat Pemulihan Bencana wajib menempatkan Sistem Elektronik pada Pusat	Pelanggan harus menempatkan sistem elektroniknya di pusat data dan pusat pemulihan bencana yang berlokasi di dalam wilayah Indonesia. Apabila pelanggan menempatkan sistem elektronik di pusat data yang berada di luar wilayah Indonesia, maka pelanggan wajib menyerahkan dokumen hukum seperti analisis risiko negara, pernyataan tertulis, dan perjanjian kerja sama untuk mendapatkan persetujuan dari

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			Data dan/atau Pusat Pemulihan Bencana di wilayah Indonesia. (2) Bank dapat menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia sepanjang memperoleh izin dari Otoritas Jasa Keuangan. LJKNB sebagaimana dimaksud pada ayat (1) dilarang menempatkan Sistem Elektronik pada Pusat Data dan/atau Pusat Pemulihan Bencana di luar wilayah Indonesia kecuali telah mendapatkan persetujuan dari Otoritas Jasa Keuangan.	Otoritas Jasa Keuangan (OJK). Tencent Cloud telah membangun atau menyewa pusat data di berbagai lokasi global sesuai dengan standar internasional terkait dan persyaratan keamanan setempat. Hal ini memberikan pelanggan pilihan multi-wilayah (multi-region) dan multi-zona ketersediaan (multi-availability zone), dengan tetap mematuhi ketat peraturan perundang-undangan di yurisdiksi operasi yang melindungi privasi pengguna dan keamanan data, serta secara aktif memantau perkembangan regulasi lokal. Pelanggan dapat dengan fleksibel menempatkan data dan sistem mereka di wilayah atau zona ketersediaan yang berbeda sesuai dengan kebutuhan pengembangan bisnis dan persyaratan keamanan data. Saat ini, Tencent Cloud memiliki tiga pusat data di Indonesia yang menyediakan beragam layanan komputasi awan, termasuk server awan (cloud server), basis data awan (cloud database), penyimpanan awan (cloud storage), dan lainnya. Pelanggan di Indonesia dapat memilih untuk menyimpan dan memproses data mereka secara lokal di Indonesia.
24	37	Kontinuitas Pusat Data dan Pusat Pemulihan Bencana	Bank dan LJKNB wajib memastikan bahwa Pusat Data dan/atau Pusat Pemulihan Bencana sebagaimana dimaksud dalam dapat menjamin	Pelanggan harus menetapkan kebijakan, standar, dan prosedur terkait aktivitas operasional pusat data, menerapkan kontrol akses fisik ke pusat data, serta melindungi keamanan lingkungan fisik pusat data. Hal ini bertujuan untuk memastikan bahwa pusat data dan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			kelangsungan usaha Bank dan LJKNB.	pusat pemulihan bencana mampu mendukung kelangsungan operasional bisnis. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, pusat data Tencent Cloud tersebar di berbagai wilayah global, terdiri dari wilayah dan zona ketersediaan, yang mencakup Tiongkok Daratan, kawasan Asia Pasifik, Amerika Utara, dan Eropa. Sebagai penyedia layanan komputasi awan, Tencent Cloud berkomitmen untuk menyediakan fondasi fasilitas fisik yang aman, stabil, berkelanjutan, dan andal bagi pelanggan. Saat ini, Tencent Cloud telah mengoperasikan tiga pusat data sewaan di wilayah Indonesia. Untuk memastikan ketahanan dan keamanan pusat data, Tencent Cloud telah membangun sistem manajemen yang komprehensif dan ketat yang mencakup seluruh proses, mulai dari seleksi operator pusat data, pengaturan perjanjian, hingga pengawasan berkelanjutan. Pelanggan dapat secara fleksibel dan mandiri menempatkan data serta sistem mereka di berbagai wilayah atau zona ketersediaan yang berbeda sesuai dengan kebutuhan pengembangan bisnis dan persyaratan keamanan data, guna memenuhi kebutuhan ketahanan bencana bisnis. Setiap zona ketersediaan terhubung dengan beberapa operator jaringan di titik keluar, membangun kemampuan cadangan bencana lintas wilayah pada jaringan Tencent Cloud, yang

Nomor LJKNB	Domain Bank	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
				secara efektif mengurangi dampak berkelanjutan dari gangguan jaringan publik operator. Jaringan dasar Tencent Cloud mengadopsi metode konstruksi redundansi NN, yang dikombinasikan dengan teknik rekayasa lalu lintas berbasis prioritas jalur dan keterjangkauan rute pada lapisan perutean, guna memastikan bahwa layanan jaringan tidak akan terputus akibat kegagalan perangkat tunggal. Node komputasi Tencent Cloud juga dibangun dengan skema redundansi NN. Ketika terjadi kegagalan pada satu node komputasi, penjadwal (scheduler) akan secara otomatis dan real time mengecualikan node tersebut, sehingga secara efektif menjaga ketersediaan layanan pelanggan. Dalam proses operasional pusat data, Tencent Cloud telah membangun mekanisme pemantauan dan evaluasi rutin, yang secara berkala melakukan penilaian komprehensif terhadap lingkungan fisik, kemampuan teknis, efisiensi respons layanan, serta efektivitas pengendalian risiko dari operator pusat data. Tencent Cloud melakukan audit dan pemeriksaan onsite tahunan di pusat data untuk memverifikasi kepatuhan operator terhadap persyaratan keamanan informasi yang ditetapkan oleh Tencent Cloud. Selain itu, Tencent Cloud meninjau hasil penilaian risiko ancaman dan kerentanan yang

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				dilaksanakan oleh operator layanan pusat data, guna memastikan efektivitas tindakan pengelolaan terkait. Informasi lebih lanjut terkait manajemen lingkungan fisik pusat data, kontrol akses, keamanan dan pengawasan, serta manajemen insiden di pusat data dapat merujuk pada Bab 5.3 "5.3 Operasional Teknologi Informasi", Klausul "22\3.2.1 Kebijakan terkait Pusat Data" dalam panduan ini.
N/A	43	Pengelolaan Data	(1) Bank wajib mengelola data secara efektif dalam pemrosesan data Bank untuk mendukung pencapaian tujuan bisnis Bank. (2) Pengelolaan data secara efektif sebagaimana dimaksud pada ayat (1) memperhatikan paling sedikit: a. kepemilikan dan kepengurusan data; b. kualitas data; c. sistem pengelolaan data; dan d. sumber daya pendukung pengelolaan data.	Saat melakukan aktivitas pemrosesan data, pelanggan harus mengelola data secara efektif, memperjelas kepemilikan dan tanggung jawab pengelolaan data, menjamin kualitas data, serta menyediakan sistem dan sumber daya pendukung yang diperlukan untuk manajemen data. Data Security Governance Center (DSGC) dapat membantu pelanggan secara otomatis mengelola aset data, melakukan klasifikasi, serta menilai risiko keamanan data perusahaan di cloud. Layanan ini merupakan platform operasional keamanan data yang mengintegrasikan deteksi dan klasifikasi data sensitif, pemetaan data, dan analisis akses data abnormal, serta berkolaborasi dengan berbagai kemampuan keamanan Tencent Cloud untuk membentuk jaringan perlindungan data tertutup. Hal ini membantu perusahaan memaksimalkan manfaat

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				keamanan. Dengan izin dari perusahaan, DSGC terhubung mendalam dengan berbagai jenis aset data di cloud, memperoleh informasi aset data secara real time dari dimensi inti. Berdasarkan karakteristik data, DSGC secara khusus membantu perusahaan mendeteksi data sensitif dan mengelola aset data dari perspektif keamanan. Sesuai standar klasifikasi data nasional, industri, atau perusahaan, DSGC membantu perusahaan melakukan klasifikasi data. Melalui visualisasi, perusahaan dapat melihat status keamanan aset dari berbagai dimensi seperti ikhtisar aset, klasifikasi data, hak akses akun, penyimpanan data, dan data sensitif. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud secara internal telah menetapkan standar klasifikasi dan penilaian tingkat data yang komprehensif. Data diklasifikasikan dan dinilai secara seragam sesuai standar ini sejak awal pembuatannya. Data pelanggan di dalam Tencent Cloud termasuk dalam kategori data dengan tingkat keamanan tinggi. Bagi karyawan internal Tencent Cloud, kecuali layanan yang dipilih pelanggan memerlukan pemrosesan data pelanggan, karyawan Tencent Cloud tidak akan berusaha mengakses data pelanggan apa pun. Dalam hal perlindungan penyimpanan data, berbagai produk

Nomor LJKNB	Domain Bank	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
				penyimpanan dan basis data Tencent Cloud mendukung fungsi enkripsi data. Layanan ini menggunakan algoritma enkripsi yang aman dan kuat, serta mengintegrasikan Key Management Service (KMS) untuk mengelola siklus hidup kunci secara menyeluruh, sehingga menjamin kerahasiaan data. Key Management System (KMS) menggunakan Hardware Security Module (HSM) yang bersertifikasi FIPS-140-2 untuk menghasilkan dan melindungi kunci, serta mampu mendukung pengelolaan siklus hidup lengkap kunci enkripsi pelanggan. Dalam hal perlindungan transmisi data, komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Antarmuka API cloud yang disediakan oleh produk-produk cloud Tencent Cloud juga dilengkapi dengan kemampuan keamanan seperti enkripsi HTTPS, verifikasi tanda tangan, dan pemantauan status, memberikan jaminan keamanan komunikasi pada tingkat port untuk bisnis pelanggan. Selain itu, pelanggan dapat menggunakan layanan Tencent Cloud berikut untuk mencapai transmisi data yang aman dalam berbagai skenario: • Direct Connect (DC) : Menyediakan koneksi jaringan pita lebar dengan keamanan tinggi dan

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				husus untuk pelanggan. Pelanggan memiliki jalur jaringan eksklusif tanpa risiko kebocoran data. • VPN Connection: Berdasarkan teknologi terowongan jaringan, layanan ini mewujudkan transmisi aman antara pusat data lokal dan sumber daya di Tencent Cloud. Terowongan VPN menggunakan IKE (Internet Key Exchange Protocol) dan IPsec untuk mengenkripsi data yang ditransmisikan, membangun saluran data yang aman dan terpercaya di internet, sehingga menjaga keamanan data selama proses transmisi.
30	44	Pelindungan Data Pribadi	(1) Bank wajib melaksanakan prinsip perlindungan data pribadi dalam melakukan pemrosesan data pribadi. (2) Dalam hal terdapat kondisi tertentu yang berpotensi meningkatkan risiko bagi pemilik data pribadi, Bank wajib melakukan penilaian dampak atas penerapan prinsip perlindungan data pribadi sebagaimana dimaksud pada ayat (1).	Saat menangani data pribadi, pelanggan harus mematuhi prinsip perlindungan data pribadi. Dalam kondisi tertentu, pelanggan perlu melaksanakan Penilaian Dampak Privasi Data Pribadi. Selain itu, dalam aktivitas pertukaran data, pelanggan harus menerapkan persyaratan perlindungan data pribadi, mengklasifikasikan data pribadi, memperjelas hak dan kewajiban pihak terkait yang terlibat dalam pertukaran data pribadi, menyusun perjanjian pertukaran data pribadi untuk mengonfirmasi metode pertukaran, serta memberikan jaminan keamanan atas data pribadi. Pelanggan harus memastikan bahwa persetujuan dari pelanggan dan calon pelanggan telah diperoleh sebelum melakukan pertukaran data pribadi.

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			Dalam menyelenggarakan Teknologi Informasi, LJKNB wajib menjamin: a. perolehan, pengolahan, penggunaan, penyimpanan, pembaruan, dan/atau pengungkapan data pribadi konsumen dilakukan berdasarkan persetujuan konsumen yang bersangkutan, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan; dan b. penggunaan atau pengungkapan data pribadi konsumen sesuai dengan tujuan yang disampaikan kepada konsumen pada saat perolehan data.	Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud menyediakan Kebijakan Privasi daring yang secara jelas menyatakan bahwa Tencent Cloud akan memproses data sesuai dengan hukum dan peraturan yang berlaku selama penyediaan layanan Tencent Cloud serta dalam situasi lainnya. Berdasarkan hal ini, Tencent Cloud menganggap kepatuhan data pribadi sebagai faktor utama dalam proses penyediaan layanan, dan menjadikan prinsip-prinsip kepatuhan data pribadi yang diakui secara umum (seperti legalitas, keadilan, transparansi, pembatasan tujuan, minimalisasi data, integritas, akurasi, kerahasiaan, akuntabilitas, dll.) sebagai panduan kepatuhan privasi. Prinsip-prinsip ini diintegrasikan ke dalam setiap tahap desain dan pengembangan produk serta sepanjang siklus hidup data pribadi, menjadikan kepatuhan privasi sebagai atribut inheren dari produk. Selain itu, Tencent Cloud secara ketat mematuhi undang-undang perlindungan privasi di berbagai negara dan wilayah yang berlaku, dengan fokus utama pada manajemen siklus hidup lengkap data pribadi, serta mengintegrasikan persyaratan kepatuhan kunci seperti Privasi by Design (PbD), respons terhadap hak subjek data, dan pengungkapan data pribadi. Pengalaman dan akumulasi keamanan Tencent Cloud selama bertahun-tahun telah memastikan keamanan infrastruktur platform
N/A	45	Pertukaran Data	(1) Dalam menerapkan perlindungan data pribadi pada kegiatan pertukaran data, Bank wajib menetapkan paling sedikit: a. klasifikasi data yang merupakan data pribadi;	

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
			b. hak dan kewajiban para pihak yang terlibat dalam pertukaran data pribadi; c. perjanjian pertukaran data pribadi; d. sarana pertukaran data pribadi; dan e. keamanan data pribadi. (2) Pertukaran data pribadi sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan persetujuan nasabah dan/atau calon nasabah yang dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.	cloud dan memberikan fondasi yang kuat untuk kepatuhan privasi bisnis pelanggan. Tencent Cloud secara internal telah menetapkan standar klasifikasi dan penilaian tingkat data yang komprehensif. Data diklasifikasikan dan dinilai secara seragam sesuai standar ini sejak awal pembuatannya. Data pelanggan di dalam Tencent Cloud termasuk dalam kategori data dengan tingkat keamanan tinggi. Bagi karyawan internal Tencent Cloud, kecuali layanan yang dipilih pelanggan memerlukan pemrosesan data pelanggan, karyawan Tencent Cloud tidak akan berusaha mengakses data pelanggan apa pun. Tencent Cloud telah memastikan akurasi data yang ditransmisikan melalui layanannya dengan menerapkan kontrol akses, verifikasi integritas, dan langkah-langkah lainnya. Selain itu, Tencent Cloud juga menyediakan saluran komunikasi bagi pelanggan, memungkinkan mereka untuk memperbaiki atau menghapus data yang tidak akurat secara mandiri. Saat memperoleh persetujuan pelanggan untuk pemrosesan data, Tencent Cloud bertindak sebagai pengendali data (data controller) dengan mengumpulkan informasi yang diberikan pelanggan saat mendaftar layanan Tencent Cloud melalui situs web resmi, serta data yang dihasilkan selama interaksi dengan Tencent Cloud dalam proses tersebut. Dalam situasi ini, Tencent

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				Cloud akan memenuhi kewajiban sebagai pengendali data sesuai dengan Kebijakan Privasi-nya. Sebagai pemroses data (data processor), pelanggan menggunakan produk atau layanan Tencent Cloud untuk memproses data yang dikumpulkan sesuai dengan tujuan bisnis mereka sendiri. Dalam hal ini, Tencent Cloud tidak hanya bertanggung jawab atas fungsionalitas dan keamanan produk atau layanan, tetapi juga memenuhi kewajiban terkait sebagai pemroses data berdasarkan Perjanjian Privasi dan Keamanan Data. Komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Antarmuka API cloud yang disediakan oleh produk-produk cloud Tencent Cloud juga dilengkapi dengan kemampuan keamanan seperti enkripsi HTTPS, verifikasi tanda tangan, dan pemantauan status, memberikan jaminan keamanan komunikasi pada tingkat port untuk bisnis pelanggan.
31	60	Laporan Insidentil	(1) Dalam hal terjadi insiden TI yang berpotensi dan/atau telah mengakibatkan kerugian yang signifikan dan/atau mengganggu kelancaran operasional Bank dan LJKNB, Bank dan LJKNB wajib menyampaikan:	Pelanggan harus melaporkan insiden teknologi informasi yang berpotensi menyebabkan kerugian besar atau mengganggu operasional kepada Otoritas Jasa Keuangan melalui saluran elektronik dalam waktu 24 jam setelah mengetahuinya, dan mengajukan laporan tertulis selambat-lambatnya dalam 5 hari kerja. Dalam hal komunikasi dan

Nomor LJKNB	Domain Bank	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			a. notifikasi awal paling lama 24 (dua puluh empat) jam setelah insiden TI diketahui; dan b. laporan insiden TI paling lama 5 (lima) hari kerja setelah insiden TI diketahui. (2) Notifikasi awal sebagaimana dimaksud pada ayat (1) huruf a disampaikan melalui sarana elektronik secara tertulis kepada Otoritas Jasa Keuangan berdasarkan informasi awal yang tersedia.	pemberitahuan insiden, Tencent Cloud telah menetapkan standar manajemen insiden keamanan informasi dan membangun prosedur terkait seperti respons insiden keamanan informasi, eskalasi insiden, serta pemberitahuan insiden. Hal ini bertujuan untuk memberikan peringatan atau pemberitahuan tepat waktu kepada pihak internal perusahaan, pelanggan, dan pemangku kepentingan lainnya yang mungkin atau telah terkena dampak insiden, sehingga memastikan semua pihak dapat berkomunikasi dan berkoordinasi secara tertib, cepat, dan efisien. Untuk insiden keamanan yang berpotensi memengaruhi pelanggan, Tencent Cloud akan menilai cakupan dan tingkat dampak insiden keamanan informasi, kemudian setelah melalui tinjauan internal, hasil penanganan dan analisis insiden tersebut akan disampaikan kepada pelanggan melalui saluran yang sesuai. Dukungan teknis juga akan disediakan untuk membantu pelanggan mengambil langkah perbaikan guna meminimalkan kerugian. Dalam hal pelanggan melaporkan masalah atau menghubungi Tencent Cloud secara aktif, konsol resmi Tencent Cloud menyediakan layanan tiket yang mendukung

Nomor		Domain	Ringkasan	Respons Tencent Cloud
LJKNB	Bank	Kontrol	Persyaratan Kontrol	
				pelanggan untuk melaporkan gangguan, insiden, masalah, dan keluhan terkait keamanan, ketersediaan, dan kerahasiaan. Tencent Cloud menyediakan layanan pelanggan online dan saluran telepon melalui konsol cloud serta situs web resminya untuk mendukung pelanggan dalam memberikan umpan balik terkait masalah yang dihadapi saat menggunakan layanan Tencent Cloud. Tencent Cloud memiliki pusat layanan pelanggan dengan cadangan lintas wilayah yang mampu menangani permintaan pelanggan secara non-stop 7*24 jam, menyediakan dukungan teknis sepanjang waktu untuk produk cloud, serta respons dan penanganan layanan yang tepat waktu dan berkualitas tinggi. Pelanggan juga dapat memilih paket layanan yang sesuai untuk mendapatkan dukungan eksklusif yang terdiri dari grup dukungan khusus, manajer layanan teknis khusus, layanan bernilai tambah, dan komponen lainnya.

07

Bagaimana Tencent Cloud Mematuhi dan Membantu Pelanggan Memenuhi Tentang Ketahanan dan Keamanan Siber Bagi Bank Umum

Seiring dengan penerapan teknologi informasi secara masif, salah satu risiko potensial yang muncul adalah ancaman siber dan risiko yang ditimbulkan oleh insiden siber. Bank tidak hanya perlu memastikan sistem elektroniknya terlindungi dari serangan siber, tetapi juga harus memiliki kemampuan untuk mendeteksi dan memulihkan diri setelah terjadinya insiden siber. Oleh karena itu, Otoritas Jasa Keuangan Indonesia menetapkan dan menerbitkan [NOMOR 29 /SEOJK.03/2022 Tentang Ketahanan dan Keamanan Siber Bagi Bank Umum](#), guna membimbing bank dalam membangun sistem operasional yang matang dan aman. Lampiran Ib: Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber dan Lampiran Ic: Penilaian Kualitas Penerapan Proses Ketahanan Siber di dalamnya memperjelas bahwa bank harus menerapkan tata kelola dan manajemen risiko yang baik, memastikan kelangsungan operasi melalui pemanfaatan teknologi informasi yang tepat, serta menjamin keamanan dan ketahanan siber. Persyaratan klausul terutama berfokus pada kerangka kerja manajemen risiko keamanan siber, proses manajemen risiko keamanan siber, kecukupan sumber daya manusia, proses identifikasi aset, ancaman, dan kerentanan, proses perlindungan aset, proses deteksi insiden siber, serta proses respons dan pemulihan insiden siber.

Dalam bab ini, Tencent Cloud akan menyaring dan merangkum persyaratan kontrol terkait penyedia layanan cloud yang tercantum dalam Lampiran Ib dan Ic dari NOMOR 29 /SEOJK.03/2022, serta menjelaskan bagaimana Tencent Cloud, sebagai penyedia layanan cloud, dapat membantu bank umum mematuhi persyaratan terkait.

7.1 Penilaian Kualitas Penerapan Manajemen Risiko terkait Keamanan Siber

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
1.3	Budaya dan Kesadaran Risiko terkait Keamanan Siber	1.3.c. Bank memastikan efektivitas pemahaman dan penerapan kebijakan keamanan siber bagi seluruh pegawai dan pemangku kepentingan terkait.	Pelanggan harus memastikan bahwa seluruh karyawan dan pemangku kepentingan memahami serta melaksanakan kebijakan keamanan siber dengan efektif. Guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Tencent Cloud secara internal juga telah membangun mekanisme pelatihan keamanan informasi, yang menyediakan berbagai kursus pelatihan bagi karyawan. Materi pelatihan mencakup aspek-aspek seperti kesadaran keamanan dasar, keamanan kantor, identifikasi dan pertahanan kerentanan, perlindungan privasi, tanggap darurat, standar keamanan pengembangan, serta persyaratan keamanan data.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
2.1	Strategi Manajemen Risiko terkait Keamanan Siber	a. Bank merumuskan strategi manajemen risiko terkait keamanan siber yang sepadan dengan kerentanan dan tingkat eksposur Bank terhadap ancaman siber serta sejalan dengan tingkat risiko yang akan diambil (risk appetite) dan toleransi risiko (risk tolerance) terkait keamanan siber serta strategi bisnis secara keseluruhan.	Pelanggan harus menetapkan strategi manajemen risiko keamanan siber yang memperjelas peran dan tanggung jawab keamanan siber, sesuai dengan toleransi dan preferensi risiko perusahaan, serta selaras dengan strategi perusahaan. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud secara internal telah menetapkan prosedur manajemen risiko keamanan informasi. Prosedur ini secara jelas mendefinisikan aktivitas seperti identifikasi risiko, analisis risiko, penyusunan rencana penanganan risiko, serta pelacakan dan pemantauan risiko. Tencent Cloud secara berkala melakukan penilaian risiko, mengidentifikasi risiko berdasarkan skenario risiko serta alur proses bisnis, produk, atau layanan. Terhadap risiko yang telah diidentifikasi, Tencent Cloud akan mengevaluasi kemungkinan terjadinya dan tingkat dampak setiap risiko untuk menentukan tingkat risiko, serta mengambil tindakan lanjutan yang sesuai. Seluruh aktivitas proses ini tercatat dengan baik. Tencent Cloud juga secara berkelanjutan melakukan tindak lanjut terhadap penanganan risiko, menilai risiko residual, dan memastikan bahwa pihak yang bertanggung jawab telah mengelola risiko dengan tepat sesuai dengan persyaratan manajemen risiko Tencent Cloud. Selain itu, berdasarkan tren perubahan industri cloud dan praktik manajemen internal, Tencent Cloud secara terus-menerus
		b. Bank memastikan kejelasan seluruh peran dan tanggung jawab terkait keamanan siber dalam strategi manajemen risiko terkait keamanan siber.	

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			memelihara dan merevisi metode penilaian risiko serta register risiko.
2.3	Kecukupan Kebijakan, Prosedur Keamanan Siber	c. Bank melakukan internalisasi kebijakan manajemen risiko terkait keamanan siber, termasuk strategi dan tujuan manajemen risiko terkait keamanan siber, ke dalam proses bisnis pada seluruh lini bisnis dan aktivitas pendukung, termasuk kebijakan yang bersifat spesifik sesuai dengan kebutuhan lini bisnis dan aktivitas pendukung Bank. d. Bank menyusun kebijakan manajemen risiko terkait keamanan siber yang memadai. e. Bank memiliki prosedur yang merupakan turunan dari kebijakan manajemen risiko terkait keamanan siber, yang dapat berupa pengendalian yang bersifat umum pada seluruh lini bisnis dan aktivitas pendukung Bank dan kontrol yang bersifat spesifik pada masing-masing lini bisnis dan aktivitas pendukung Bank.	Pelanggan harus menetapkan kebijakan dan prosedur keamanan siber yang disesuaikan dengan karakteristik dan kompleksitas aktivitas bisnis, serta diintegrasikan ke dalam semua lini bisnis dan proses operasional pendukung. Guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi.
2.3	Pelindungan	f. Bank memiliki kebijakan	Pelanggan harus menetapkan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
	Aset	dan prosedur keamanan siber yang digunakan untuk mengatur perlindungan aset TI.	kebijakan dan prosedur keamanan siber terkait perlindungan aset TI. Pelanggan juga dapat menggunakan platform manajemen keamanan terpadu Tencent Cloud, Cloud Security Center (CSC), untuk mengelola keamanan aset informasi. CSC mencakup fungsionalitas Asset Security Center, yang membantu pelanggan dalam melakukan inventarisasi dinamis otomatis terhadap aset di cloud, termasuk server cloud, penyimpanan objek, database cloud, penyeimbang beban, dan lainnya. Melalui berbagai dimensi keamanan seperti risiko konfigurasi cloud, kerentana, dan insiden keamanan, CSC menyediakan manajemen terpadu terhadap risiko keamanan aset, sehingga mengurangi risiko "IT bayangan" (shadow IT) di cloud. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar manajemen aset informasi dan proses manajemen siklus hidup lengkap. Hal ini mencakup pengelolaan dan perlindungan aset seperti data elektronik, perangkat keras dan perangkat virtualnya, infrastruktur, sistem aplikasi, serta perangkat lunak melalui klasifikasi dan penilaian tingkat kepentingan. Tencent Cloud mengelola perangkat keras dan komponen perangkat lunak menggunakan sistem manajemen aset, yang meliputi pendaftaran dan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pengikatan aset, inventarisasi dan pembaruan informasi aset, serta pensiun dan penggantian aset. Tujuannya adalah untuk memastikan operasi yang stabil dari sistem dasar platform cloud dan memberikan dukungan yang andal bagi sistem bisnis.
2.3	Pihak Ketiga	g. Bank memiliki kebijakan dan prosedur manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga yang mengatur tentang pengelolaan data/informasi digital milik Bank (termasuk data nasabah yang dimiliki Bank) oleh pihak ketiga dan subkontraktor dari pihak ketiga. h. Bank menerapkan manajemen risiko terkait keamanan siber untuk pihak ketiga dan subkontraktor dari pihak ketiga. i. Bank menetapkan standar minimum kendali keamanan siber bagi pihak ketiga dan subkontraktor dari pihak ketiga, yaitu: 1) ketentuan kerahasiaan di kontrak kerja sama; 2) ketersediaan tata kelola pengamanan siber di pihak ketiga dan subkontraktor dari pihak	Pelanggan harus menetapkan kebijakan dan prosedur manajemen keamanan siber untuk pihak ketiga dan subkontraktornya, yang mencakup klausul kerahasiaan dalam perjanjian kerja sama, serta mensyaratkan pihak ketiga dan subkontraktornya memiliki mekanisme tata kelola keamanan siber dan melaksanakan manajemen risiko keamanan siber. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti KETENTUAN LAYANAN, General Service Level Agreement, Perjanjian Privasi dan Keamanan Data, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. Guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		ketiga (kebijakan, prosedur, ketentuan, dan lainnya); dan 3) pengelolaan risiko terkait keamanan siber termasuk manajemen insiden siber di pihak ketiga dan subkontraktor dari pihak ketiga.	menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Tim keamanan Tencent Cloud secara berkelanjutan memantau dan mengevaluasi risiko keamanan internal untuk menjaga efektivitas dan keandalan sistem manajemen keamanan informasi. Tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun, dan secara terus-menerus memantau kondisi platform cloud dan sistem internal, memastikan bahwa mereka mempertahankan postur keamanan yang baik dan mematuhi peraturan dan persyaratan standar manajemen keamanan serta peraturan perundang-undangan yang berlaku. Selain itu, Tencent Cloud juga menjalani audit profesional oleh pihak ketiga independen setiap tahun. Melalui laporan Sistem dan Kontrol

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			Organisasi (SOC) yang bersifat asersi, Tencent Cloud mengungkapkan kondisi terkini pengendalian internal organisasi layanannya kepada lembaga pengguna cloud, auditor independen, regulator, pemegang saham perusahaan, serta pihak-pihak terkait lainnya. Untuk skenario penanganan subkontrak, perjanjian juga mencakup klausul seperti persetujuan sebelumnya untuk subkontrak, pemberitahuan sebelum penambahan atau penggantian subkontrak, serta kewajiban perlindungan data. Tanpa persetujuan sebelumnya dari pelanggan, Tencent Cloud tidak akan mensubkontrakkan operasi pemrosesan apa pun yang dilaksanakan atas nama pelanggan berdasarkan kontrak/perjanjian. Setiap perubahan yang diantisipasi terkait penambahan atau penggantian pihak subkontrak pemrosesan akan diberitahukan kepada pelanggan melalui saluran seperti email. Selain itu, pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut. Dalam hal manajemen subkontraktor, Tencent Cloud telah membangun sistem manajemen keamanan rantai pasok yang komprehensif. Melalui evaluasi dan persetujuan keamanan pemasok yang ketat, pemantauan dan penilaian berkala, serta perjanjian layanan outsourcing yang jelas, Tencent Cloud melakukan kontrol

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			efektif terhadap pemasok. Hal ini memastikan bahwa subkontrak tidak memengaruhi kemampuan Tencent Cloud dalam menyediakan layanan terkait kepada pelanggan, kerahasiaan dan integritas proses penanganan informasi pelanggan, serta hak pengawasan dan audit dari otoritas pengawas keuangan dan lembaga keuangan Indonesia. Tencent Cloud akan secara aktif mendukung persyaratan manajemen outsourcing pelanggan, serta responsif dan kooperatif dalam menghadapi audit atau kegiatan penilaian yang dimulai oleh pihak pelanggan.
3.1	Proses Manajemen Risiko terkait Keamanan Siber (Identifikasi, Pengukuran, Pemantauan, dan Pengendalian)	a. Bank melaksanakan identifikasi seluruh risiko terkait keamanan siber secara berkala. b. Bank memastikan tersedianya metode atau sistem untuk melakukan identifikasi risiko pada seluruh kegiatan Bank yang terkait dengan keamanan siber. c. Bank melakukan pengukuran risiko secara berkala untuk seluruh kegiatan Bank yang terkait dengan keamanan siber. f. Bank memiliki sistem dan prosedur pemantauan risiko terkait keamanan siber yang antara.	Pelanggan harus secara berkala melaksanakan penilaian risiko keamanan siber, membangun sistem terkait untuk mengidentifikasi risiko keamanan siber, melakukan pengukuran risiko terhadap aktivitas bisnis yang berkaitan dengan keamanan siber, serta menetapkan sistem dan prosedur pemantauan risiko terkait keamanan siber. Dalam rangka mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud secara internal menetapkan prosedur manajemen risiko keamanan informasi, yang secara jelas mendefinisikan dan memberikan panduan untuk seluruh proses manajemen risiko (identifikasi risiko, analisis risiko, penyusunan rencana penanganan risiko, serta pelacakan dan pemantauan risiko). • Identifikasi Risiko: Tencent Cloud

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			secara berkala melaksanakan penilaian risiko, mengidentifikasi skenario risiko yang relevan berdasarkan laporan insiden keamanan industri, pengalaman praktis Tencent Cloud, serta basis data risiko dari lembaga profesional. Identifikasi risiko dilakukan melalui analisis terhadap skenario risiko serta hasil analisis proses bisnis, produk, atau layanan. • Penilaian Risiko: Tencent Cloud mengevaluasi nilai aset, kemungkinan terjadinya risiko dalam skenario tertentu, serta tingkat dampak risiko, kemudian menghitung tingkat risiko berdasarkan parameter tersebut. • Penanganan Risiko: Berdasarkan hasil analisis risiko, Tencent Cloud menerapkan strategi respons dan langkah-langkah mitigasi yang sesuai untuk setiap risiko yang teridentifikasi. Untuk risiko tinggi, penanggung jawab risiko menyusun rencana penanganan (melalui transfer risiko atau tindakan pengurangan risiko) dan memperbarui tabel manajemen risiko. Untuk risiko sedang, penanggung jawab risiko menilai kebutuhan penyusunan rencana penanganan berdasarkan kondisi aktual. Untuk risiko rendah, risiko tersebut dianggap dapat diterima. Tencent Cloud juga secara berkala meninjau risiko residual untuk memantau status dan nilai

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			risikonya. • Pemantauan, Tinjauan, dan Pelaporan Risiko: Tencent Cloud mengumpulkan hasil penilaian risiko, menghasilkan laporan penilaian risiko, dan menyampaikannya kepada manajemen. Selain itu, Tencent Cloud memelihara tabel manajemen risiko, memantau perubahan kondisi risiko serta status rencana penanganan risiko, dan menyesuaikan rencana manajemen risiko secara real time. Selain itu, Tencent Cloud mendefinisikan indikator risiko kunci dan secara berkala melakukan pengukuran terhadap indikator tersebut. Dengan membandingkannya terhadap kriteria risiko yang dapat diterima, Tencent Cloud menganalisis akar penyebab masalah yang ditemukan serta mengusulkan rekomendasi dan solusi perbaikan.
3.2	Kecukupan SDM terkait Keamanan Siber	b. Direksi mengembangkan sistem penerimaan, pengembangan, dan pelatihan pegawai, termasuk rencana suksesi manajerial serta remunerasi yang memadai untuk memastikan tersedianya pegawai yang kompeten di bidang manajemen risiko terkait keamanan siber. c. Direksi memastikan	Pelanggan harus membangun sistem rekrutmen, pengembangan, dan pelatihan personel untuk mengelola staf secara tepat. Langkah-langkah ini mencakup pembentukan proses seleksi personel, penandatanganan perjanjian kerahasiaan dengan karyawan, serta penyelenggaraan mekanisme manajemen sosialisasi kesadaran risiko teknologi informasi. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan standar dan prosedur manajemen sumber daya manusia

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		bahwa seluruh SDM memiliki pemahaman yang memadai atas risiko terkait keamanan siber dan mampu mengomunikasikan implikasi risiko terkait keamanan siber kepada Direksi, Dewan Komisaris, manajemen, dan nasabah. d. Direksi memastikan agar seluruh SDM memahami strategi, tingkat risiko terkait keamanan siber yang akan diambil (risk appetite) dan toleransi risiko (risk tolerance) terkait keamanan siber, kerangka manajemen risiko terkait keamanan siber yang telah ditetapkan oleh Direksi dan disetujui oleh Dewan Komisaris, serta memastikan seluruh SDM menerapkannya secara konsisten dalam aktivitas yang ditangani. f. Bank mengembangkan dan mengimplementasikan program berkelanjutan untuk peningkatan kapasitas terkait keamanan siber kepada seluruh pegawai yang relevan, termasuk level Direksi, Dewan Komisaris, dan manajemen untuk memastikan bahwa setiap	yang komprehensif, guna memastikan seleksi, perekrutan, dan penempatan personel sesuai dengan persyaratan posisi. Tencent Cloud membangun prosedur manajemen siklus hidup karyawan yang jelas, meliputi proses penerimaan, periode kerja, dan proses pemberhentian. Sebelum Penerimaan: Pelamar akan menjalani wawancara, di mana Tencent Cloud menilai apakah kompetensi mereka memenuhi persyaratan posisi. Berdasarkan hukum yang berlaku dan tingkat posisi, departemen SDM melakukan pemeriksaan latar belakang kandidat sebelum penugasan. Pemeriksaan ini mencakup riwayat pekerjaan sebelumnya, latar belakang kriminal, dan verifikasi pendidikan. Hasil pemeriksaan dicatat dalam sistem manajemen SDM Tencent Cloud. Setelah Penerimaan: Karyawan internal wajib menandatangani Perjanjian Penugasan (Assignment Agreement) dan Perjanjian Kerahasiaan (Non-Disclosure Agreement). Perjanjian Penugasan menjelaskan kebijakan keamanan yang berlaku di Tencent Cloud, serta tanggung jawab karyawan atau pihak ketiga dalam melindungi keamanan informasi dan data pribadi. Sementara Perjanjian Kerahasiaan mencakup kewajiban dan tanggung jawab kerahasiaan penandatanganan, serta konsekuensi yang mungkin diterima jika melanggar klausul kerahasiaan. Karyawan outsourcing juga harus

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		pegawai memiliki kompetensi dan keahlian untuk menjalankan peran dan tanggung jawab secara efektif. g. Bank melakukan analisis kesenjangan (gap analysis) untuk memahami tingkat pengetahuan dan kemampuan pegawai terkait keamanan siber dan menggunakan informasi tersebut untuk membuat rencana aksi peningkatan kapasitas pegawai.	menjalani pemeriksaan latar belakang sebelum penugasan dan tunduk pada ketentuan penugasan serta kerahasiaan yang diatur dalam perjanjian antara Tencent Cloud dan penyedia outsourcing. Persyaratan kerahasiaan antara Tencent Cloud dengan karyawan dan pihak ketiga ditinjau dan diperbarui oleh departemen hukum sesuai kebutuhan. Dalam hal pelatihan dan sosialisasi kesadaran keamanan informasi, Tencent Cloud secara internal telah membangun mekanisme pelatihan keamanan informasi yang komprehensif. Tencent Cloud mewajibkan karyawan tetap, konsultan, magang, dan karyawan outsourcing untuk mengikuti kursus pelatihan keamanan informasi. Kursus-kursus terkait mencakup pelatihan wajib untuk semua staf, pelatihan khusus untuk posisi kunci, serta pelatihan mata pelajaran pilihan. Materi yang diajarkan meliputi aspek-aspek seperti kesadaran keamanan dasar, keamanan kantor, identifikasi dan pertahanan kerentanan, perlindungan privasi, tanggap darurat, standar keamanan pengembangan, dan persyaratan keamanan data.
4.2	Kaji Ulang dan Evaluasi	a. Bank melakukan kaji ulang dan evaluasi terhadap penerapan manajemen risiko terkait keamanan siber secara berkala sesuai dengan karakteristik dan kompleksitas Bank.	Pelanggan harus membangun mekanisme audit teknologi informasi, secara berkala melakukan tinjauan dan evaluasi terhadap pelaksanaan manajemen risiko keamanan siber, serta memastikan bahwa auditor memiliki kompetensi dan keterampilan profesional. Hasil tinjauan dan evaluasi tersebut harus

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		b. Bank memastikan satuan kerja yang menjalankan fungsi manajemen risiko terkait keamanan siber melakukan kaji ulang dan evaluasi secara memadai.	dilaporkan kepada manajemen. Tim keamanan Tencent Cloud secara berkelanjutan melakukan pemantauan dan penilaian terhadap risiko keamanan internal untuk memastikan efektivitas dan keandalan sistem manajemen keamanan informasi.
		c. Bank memastikan satuan kerja audit intern melakukan kaji ulang dan evaluasi secara memadai.	Selain itu, tim keamanan Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun dan terus memantau kondisi platform cloud serta sistem internal untuk memastikan postur keamanan yang baik, sesuai dengan ketentuan dan persyaratan peraturan perundang-undangan serta standar manajemen keamanan yang berlaku. Tencent Cloud juga menjalani audit profesional oleh pihak ketiga independen setiap tahun. Melalui laporan Sistem dan Kontrol Organisasi (SOC) yang bersifat asersi, Tencent Cloud mengungkapkan kondisi terkini pengendalian internal organisasi layanannya kepada lembaga pengguna cloud, auditor independen, regulator, pemegang saham perusahaan, serta pihak-pihak terkait lainnya.
		d. Bank memastikan pihak yang melakukan kaji ulang dan evaluasi atas penerapan manajemen risiko terkait keamanan siber memiliki independensi dan kompetensi yang baik serta metode kaji ulang yang andal.	
		e. Bank memastikan bahwa hasil kaji ulang dan evaluasi atas penerapan manajemen risiko terkait keamanan siber telah disampaikan kepada Direksi dan Dewan Komisaris untuk diambil langkah perbaikan dan/atau penyempurnaan manajemen risiko terkait keamanan siber.	Untuk memastikan kebijakan, prosedur, proses, dan langkah pengendalian teknologi informasi Tencent Cloud memenuhi persyaratan regulasi keuangan Indonesia, Tencent Cloud telah lolos audit kepatuhan IT industri keuangan Indonesia yang dilakukan oleh pihak ketiga independen dan sertifikasi SNI 27001. Pelanggan dapat mengunduh laporan terbaru secara mandiri dari Pusat

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
-------	----------------	-------------------------------	-----------------------

[Dokumen Kepatuhan Tencent Cloud.](#)

7.2 Penilaian Kualitas Penerapan Proses Ketahanan Siber

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
1.a	Pelindungan Aset	a. Bank menerapkan manajemen aset melalui inventarisasi dan penilaian aset TI (antara lain perangkat keras, perangkat lunak, jaringan, dan infrastruktur) serta pencatatan konfigurasi secara efektif.	Pelanggan harus melakukan inventarisasi dan evaluasi efektif terhadap aset TI, serta mencatat informasi konfigurasinya. Pelanggan juga dapat menggunakan platform manajemen keamanan terpadu Tencent Cloud, Cloud Security Center (CSC), untuk mengelola keamanan aset informasi. CSC mencakup fungsionalitas Asset Security Center, yang membantu pelanggan dalam melakukan inventarisasi dinamis otomatis terhadap aset di cloud, termasuk server cloud, penyimpanan objek, database cloud, penyeimbang beban, dan lainnya. Melalui berbagai dimensi keamanan seperti risiko konfigurasi cloud, kerentana, dan insiden keamanan, CSC menyediakan manajemen terpadu terhadap risiko keamanan aset, sehingga mengurangi risiko "IT bayangan" (shadow IT) di cloud. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			menetapkan standar manajemen aset informasi dan proses manajemen siklus hidup lengkap. Hal ini mencakup pengelolaan dan perlindungan aset seperti data elektronik, perangkat keras dan perangkat virtualnya, infrastruktur, sistem aplikasi, serta perangkat lunak melalui klasifikasi dan penilaian tingkat kepentingan. Tencent Cloud mengelola perangkat keras dan komponen perangkat lunak menggunakan sistem manajemen aset, yang meliputi pendaftaran dan pengikatan aset, inventarisasi dan pembaruan informasi aset, serta pensiun dan penggantian aset. Tujuannya adalah untuk memastikan operasi yang stabil dari sistem dasar platform cloud dan memberikan dukungan yang andal bagi sistem bisnis.
1.b	Kerentanan	b. Bank melakukan identifikasi kerentanan dan pemantauan terhadap perkembangan siber terkini untuk mengidentifikasi ancaman siber.	Pelanggan harus mengidentifikasi kerentanan dan mendeteksi perkembangan terbaru dalam dinamika jaringan, serta mengenali ancaman siber. Dalam hal pemindaian kerentanan, pelanggan dapat memilih <u>Vulnerability Scanning Service (VSS)</u> untuk mendeteksi aset jaringan perusahaan dan mengidentifikasi risikonya. Berdasarkan pengalaman keamanan dan intelijen ancaman yang dikumpulkan Tencent selama bertahun-tahun, VSS telah membangun basis aturan kerentanan yang kaya dan komprehensif, serta memiliki kemampuan deteksi kerentanan 0Day/1Day/NDay yang profesional dan efisien. Layanan ini

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			dapat melakukan pemindaian keamanan berkala, peringatan risiko berkelanjutan, dan deteksi kerentanan terhadap ketersediaan, keamanan, serta kepatuhan aset pelanggan, sekaligus memberikan rekomendasi perbaikan yang profesional untuk mengurangi risiko keamanan. VSS juga mendukung integrasi dengan produk cloud seperti Host Security dan Web Application Firewall, mencapai siklus tertutup dari pemantauan risiko hingga penanganan risiko. Untuk mendukung pelanggan dalam mendeteksi dan menganalisis ancaman, Tencent Cloud menyediakan Threat Intelligence Center (TIX). Sebagai platform layanan intelijen terpadu, TIX menyediakan tiga kemampuan intelijen utama: intelijen dasar, intelijen permukaan serangan, dan intelijen bisnis. Platform ini mendukung fungsi seperti kueri intelijen, analisis dan penilaian IOC, serta manajemen permukaan serangan. Kemampuan ini membantu pelanggan menganalisis dan menilai insiden keamanan dengan lebih efisien, serta menilai risiko paparan aset perusahaan secara lebih komprehensif, sehingga mendukung pembangunan sistem pertahanan keamanan multidimensi yang efektif. TIX membangun jaringan titik kontak intelijen yang lengkap, mengumpulkan dan menganalisis intelijen ancaman dari berbagai

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			sumber seperti komunitas kerentanan, lembaga keamanan, penyedia alat keamanan, media sosial, dan blog keamanan. Platform ini juga terintegrasi dengan algoritma dan daya komputasi cloud untuk menghilangkan alarm palsu, sehingga memastikan keakuratan intelijen. Selain itu, Threat Intelligence Center berfokus pada model layanan SaaS, mendukung berbagai metode pengiriman seperti API berbasis web, SDK, TIP, dan mini-program untuk memenuhi kebutuhan pelanggan yang beragam. Threat Intelligence Center juga dapat diintegrasikan dengan produk perlindungan keamanan yang sudah dimiliki pelanggan, sehingga data intelijen dari cloud dapat dikaitkan untuk meningkatkan efisiensi operasi keamanan dan respons ancaman secara keseluruhan.
1.c	Pengujian Keamanan Siber	c. Bank melakukan pengujian keamanan siber secara berkala.	Pelanggan harus secara berkala melaksanakan pengujian keamanan siber. Dalam hal pengujian penetrasi, Tencent Cloud menyediakan layanan <u>Penetration Testing Service (PTS)</u> bagi pelanggan. Layanan ini sepenuhnya mensimulasikan teknik serangan dan deteksi kerentanan yang mungkin digunakan oleh peretas, dengan menerapkan metode dan pendekatan yang terkendali serta non-destruktif untuk melakukan pemeriksaan mendalam terhadap keamanan sistem target. Hal ini membantu mengidentifikasi kelemahan dalam target dan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			perangkat jaringan, memberikan rekomendasi penguatan keamanan untuk meningkatkan keamanan sistem pelanggan, serta mendukung verifikasi setelah perbaikan kerentanan dilakukan. Dalam hal pemindaian kerentanan, pelanggan dapat memilih Vulnerability Scanning Service (VSS) untuk mendeteksi aset jaringan perusahaan dan mengidentifikasi risikonya. Berdasarkan pengalaman keamanan dan intelijen ancaman yang dikumpulkan Tencent selama bertahun-tahun, VSS telah membangun basis aturan kerentanan yang kaya dan komprehensif, serta memiliki kemampuan deteksi kerentanan 0Day/1Day/NDay yang profesional dan efisien. Layanan ini dapat melakukan pemindaian keamanan berkala, peringatan risiko berkelanjutan, dan deteksi kerentanan terhadap ketersediaan, keamanan, serta kepatuhan aset pelanggan, sekaligus memberikan rekomendasi perbaikan yang profesional untuk mengurangi risiko keamanan. VSS juga mendukung integrasi dengan produk cloud seperti Host Security dan Web Application Firewall, mencapai siklus tertutup dari pemantauan risiko hingga penanganan risiko. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud secara berkala menghasilkan tugas pemindaian melalui sistem pemindaian

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			kerentanan untuk memindai aset di lingkungan cloud, serta menganalisis, mengklasifikasikan, dan menangani kerentanan yang ditemukan. Selain itu, Tencent Cloud secara berkala melaksanakan pengujian penetrasi skala besar pada seluruh rantai layanan, guna secara proaktif mengidentifikasi dan memperbaiki potensi risiko keamanan sistem sedini mungkin. Pengujian penetrasi yang ditargetkan juga dilakukan secara fleksibel dalam situasi seperti sebelum peluncuran produk baru atau perubahan besar lainnya. Hasil pengujian penetrasi dikomunikasikan ke departemen terkait melalui tiket keamanan, dan departemen tersebut segera melakukan perbaikan kerentanan atau menerapkan langkah pengendalian kompensasi lainnya, guna memastikan kerentanan yang dieksploitasi selama pengujian penetrasi telah ditangani dengan baik. Tencent Cloud secara berkala menyelenggarakan simulasi latihan pertahanan "Tim Merah vs Tim Biru" untuk melawan serangan siber secara realistis. Tencent Cloud juga membangun platform umpan balik kerentanan eksternal dan meluncurkan "Program Penghargaan Kerentanan" yang mengundang pakar keamanan industri untuk membantu mengidentifikasi kerentanan dan risiko keamanan sistem dari perspektif peretas, sehingga masalah keamanan dapat diperbaiki tepat waktu dan keamanan ekosistem Tencent Cloud tetap terjaga.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
2.a 2.b 2.c, 2.d	Pengendalian Keamanan	a. Bank menerapkan pengendalian keamanan (security control) yang komprehensif sesuai dengan hasil identifikasi aset, ancaman, dan kerentanan. b. Bank melakukan pemeliharaan dan perbaikan terhadap pengendalian keamanan atas aset TI sesuai dengan kebijakan dan prosedur yang berlaku. c. Bank menerapkan sistem pengamanan yang dikelola dengan baik sesuai kebijakan dan prosedur yang berlaku. d. Bank melakukan penginian pengendalian keamanannya secara berkala untuk memastikan kecukupan kontrol keamanan yang digunakan sesuai dengan hasil terkini dari proses identifikasi.	Pelanggan harus menyusun langkah-langkah pengendalian keamanan siber berdasarkan hasil penilaian risiko, menerapkan sistem keamanan yang dikelola sesuai standar, serta secara berkala meninjau dan memperbarui tindakan pengendalian keamanan. Sesuai kebijakan dan prosedur yang berlaku, pelanggan perlu memastikan kecukupan tindakan pengendalian keamanan yang digunakan. Guna mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud telah menetapkan kebijakan manajemen keamanan informasi yang terdiri dari strategi keseluruhan keamanan informasi, struktur organisasi keamanan, dan sistem manajemen keamanan. Kebijakan ini secara efektif mendukung operasi yang aman dan manajemen risiko platform cloud. Kebijakan keamanan informasi Tencent Cloud ditinjau secara berkala setiap tahun untuk memastikan bahwa tujuan pengendalian, prosedur pengendalian, serta tindakan pengendalian sistem manajemen keamanan cloud sesuai dengan strategi keamanan, standar, prosedur, dan persyaratan hukum terkait, sehingga menjamin kecukupan dan efektivitas kebijakan keamanan informasi. Tim keamanan Tencent Cloud secara berkelanjutan memantau dan mengevaluasi risiko keamanan internal untuk menjaga efektivitas dan keandalan sistem manajemen keamanan informasi. Tim keamanan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			Tencent Cloud melakukan audit keamanan internal setidaknya sekali setahun, dan secara terus-menerus memantau kondisi platform cloud dan sistem internal, memastikan bahwa mereka mempertahankan postur keamanan yang baik dan mematuhi peraturan dan persyaratan standar manajemen keamanan serta peraturan perundang-undangan yang berlaku. Selain itu, Tencent Cloud juga menjalani audit profesional oleh pihak ketiga independen setiap tahun. Melalui laporan Sistem dan Kontrol Organisasi (SOC) yang bersifat asersi, Tencent Cloud mengungkapkan kondisi terkini pengendalian internal organisasi layanannya kepada lembaga pengguna cloud, auditor independen, regulator, pemegang saham perusahaan, serta pihak-pihak terkait lainnya. Untuk memastikan kebijakan, prosedur, proses, dan langkah pengendalian teknologi informasi Tencent Cloud memenuhi persyaratan regulasi keuangan Indonesia, Tencent Cloud telah lolos audit kepatuhan IT industri keuangan Indonesia yang dilakukan oleh pihak ketiga independen dan sertifikasi SNI 27001. Pelanggan dapat mengunduh laporan terbaru secara mandiri dari Pusat Dokumen Kepatuhan Tencent Cloud.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
2.e	Keamanan Data dan Informasi	e. Bank menerapkan manajemen keamanan data dan informasi serta memastikan bahwa data dan/atau informasi dikelola sesuai dengan strategi manajemen risiko terkait keamanan siber pada organisasi untuk melindungi kerahasiaan, integritas, serta ketersediaan data dan informasi.	Pelanggan harus menetapkan mekanisme perlindungan keamanan data, mengklasifikasikan data berdasarkan tingkat kepekaan dan kepentingannya, serta menerapkan langkah-langkah perlindungan data sesuai dengan tingkat data yang berbeda. Penggunaan standar enkripsi yang diakui secara internasional dan dapat dipercaya diperlukan untuk melindungi kerahasiaan dan integritas data. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Dalam hal klasifikasi dan tingkatan data, <u>Data Security Governance Center (DSGC)</u> dapat membantu pelanggan secara otomatis mengelola aset data, melakukan klasifikasi, serta menilai risiko keamanan data perusahaan di cloud. Dengan izin dari perusahaan, DSGC terhubung mendalam dengan berbagai jenis aset data di cloud, memperoleh informasi aset data secara real time dari dimensi inti. Berdasarkan karakteristik data, DSGC secara khusus membantu perusahaan mendeteksi data sensitif dan mengelola aset data dari perspektif keamanan. Sesuai standar klasifikasi data nasional, industri, atau perusahaan, DSGC membantu perusahaan melakukan klasifikasi data. Tencent Cloud secara internal telah menetapkan standar klasifikasi dan penilaian tingkat data yang

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			komprehensif. Data diklasifikasikan dan dinilai secara seragam sesuai standar ini sejak awal pembuatannya. Data pelanggan di dalam Tencent Cloud termasuk dalam kategori data dengan tingkat keamanan tinggi. Bagi karyawan internal Tencent Cloud, kecuali layanan yang dipilih pelanggan memerlukan pemrosesan data pelanggan, karyawan Tencent Cloud tidak akan berusaha mengakses data pelanggan apa pun. Dalam hal perlindungan penyimpanan data, berbagai produk penyimpanan dan basis data Tencent Cloud mendukung fungsi enkripsi data. Layanan ini menggunakan algoritma enkripsi yang aman dan kuat, serta mengintegrasikan Key Management Service (KMS) untuk mengelola siklus hidup kunci secara menyeluruh, sehingga menjamin kerahasiaan data. Key Management System (KMS) menggunakan Hardware Security Module (HSM) yang bersertifikasi FIPS-140-2 untuk menghasilkan dan melindungi kunci, serta mampu mendukung pengelolaan siklus hidup lengkap kunci enkripsi pelanggan. untuk mengurangi risiko kunci dipecahkan atau disalahgunakan, KMS mendukung rotasi kunci dan menggunakan metode yang aman serta andal untuk menghapus kunci yang telah kedaluwarsa, tidak berlaku, atau bocor. Kunci yang telah dihapus tidak dapat dipulihkan, dan data

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			terenkripsi di bawah kunci tersebut juga tidak dapat didekripsi. Selain itu, Tencent Cloud menggunakan teknologi penyimpanan redundan multi-salinan dan kode penghapusan saat menyimpan data, serta segera mengambil tindakan pemulihan yang diperlukan ketika mendeteksi kesalahan integritas, sehingga sangat meningkatkan kemampuan toleransi kesalahan data. Dalam hal perlindungan transmisi data, komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Antarmuka API cloud yang disediakan oleh produk-produk cloud Tencent Cloud juga dilengkapi dengan kemampuan keamanan seperti enkripsi HTTPS, verifikasi tanda tangan, dan pemantauan status, memberikan jaminan keamanan komunikasi pada tingkat port untuk bisnis pelanggan. Selain itu, pelanggan dapat menggunakan layanan Tencent Cloud berikut untuk mencapai transmisi data yang aman dalam berbagai skenario: • <u>Direct Connect (DC)</u>: Menyediakan koneksi jaringan pita lebar dengan keamanan tinggi dan khusus untuk pelanggan. Pelanggan memiliki jalur jaringan eksklusif tanpa risiko kebocoran data. • <u>VPN Connection</u>:Berdasarkan teknologi terowongan jaringan,

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			layanan ini mewujudkan transmisi aman antara pusat data lokal dan sumber daya di Tencent Cloud. Terowongan VPN menggunakan IKE (Internet Key Exchange Protocol) dan IPsec untuk mengenkripsi data yang ditransmisikan, membangun saluran data yang aman dan terpercaya di internet, sehingga menjaga keamanan data selama proses transmisi. Untuk penghapusan dan pemusnahan data, Tencent Cloud menyediakan mekanisme pemusnahan data yang aman dan dapat diandalkan. Setelah layanan cloud diakhiri, Tencent Cloud akan mengikuti metode penghapusan data yang ketat dan menghapus sepenuhnya data pelanggan, termasuk salinan dan cadangannya, setelah periode retensi berakhir. Data yang telah dihapus tidak dapat dipulihkan. Ketika media yang digunakan untuk menyediakan layanan Tencent Cloud mengalami kerusakan dan perlu diganti atau telah mencapai akhir masa pakai sehingga harus dibuang, Tencent Cloud juga akan segera melakukan penghancuran fisik secara menyeluruh sesuai dengan prosedur yang ketat.
2.f	Pelindungan Terhadap Jaringan, Perangkat Keras, dan Perangkat Lunak	f. Bank menerapkan manajemen perlindungan terhadap jaringan, perangkat keras, dan perangkat lunak	Pelanggan harus mengelola segmentasi jaringan berdasarkan tingkat kritis sistem atau kepekaan data, serta menerapkan dan memasang perangkat keamanan jaringan seperti firewall, sistem

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		lunak.	pencegahan intrusi, dan perlindungan DDoS. Selain itu, pelanggan juga perlu menerapkan langkah-langkah perlindungan yang diperlukan pada perangkat keras dan perangkat lunak yang digunakan oleh sistem informasi. Untuk persyaratan segmentasi atau zonasi jaringan, pelanggan dapat menggunakan layanan Virtual Private Cloud (VPC) yang disediakan oleh Tencent Cloud untuk membangun beberapa ruang jaringan independen bagi sumber daya platform cloud yang telah dibeli, serta menyesuaikan pembagian segmen jaringan, alamat IP, kebijakan perutean, dan lainnya. Layanan VPC merupakan ruang jaringan eksklusif di cloud yang dibangun berdasarkan infrastruktur Tencent Cloud. VPC menggunakan teknologi tunneling untuk membangun jaringan virtual di atas jaringan fisik dan menerapkan teknologi virtualisasi guna mencapai isolasi lengkap antara jaringan privat yang berbeda, memberikan pelanggan jaringan cloud yang aman, independen, dan terisolasi. Untuk server cloud di dalam VPC, kontrol lalu lintas masuk dan keluar pada tingkat instance dan subnet dapat diterapkan dengan mengonfigurasi aturan Security Group dan Network ACL, mencapai kontrol akses jaringan pada berbagai tingkatan. Untuk menerapkan perlindungan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			batas jaringan, Tencent Cloud menyediakan EdgeOne (EO) platform untuk pelanggan. Berbasis pada simpul global Tencent Edge, layanan ini memberikan perlindungan keamanan dan layanan percepatan kepada pelanggan, dengan kemampuan seperti perlindungan DDoS, perlindungan Web cerdas, perlindungan serangan BOT/crawler, resolusi DNS, serta dukungan bagi pelanggan untuk mengonfigurasi aturan kontrol akses kustom sesuai kebutuhan bisnis. Pelanggan juga dapat memilih alat perlindungan batas jaringan seperti Cloud Firewall, Web Application Firewall (WAF), dan Anti-DDoS. Di antaranya, Cloud Firewall (CFW) terutama menyediakan perlindungan di berbagai batas jaringan untuk pelanggan. Layanan ini mendukung fungsi seperti kontrol aktif ACL firewall, penyaringan IPS real time, patching virtual, dan deteksi kode berbahaya. Dengan kemampuan ini, CFW dapat memenuhi kebutuhan zona DMZ dalam jaringan tradisional, memberikan perlindungan fokus pada aset inti, serta mencapai kontrol isolasi granular antar VPC. Web Application Firewall (WAF) membantu pengguna di dalam maupun di luar Tencent Cloud dalam menangani masalah keamanan situs web dan layanan web, seperti

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			serangan web, intrusi, eksploitasi kerentanan, injeksi malware, pemalsuan, backdoor, dan serangan crawler. Sementara itu, Anti-DDoS mengatasi masalah serangan DDoS dengan memanfaatkan sumber daya perlindungan DDoS yang memadai dan berkualitas tinggi, dikombinasikan dengan algoritma pembersihan yang terus berkembang berbasis "teknologi mandiri + identifikasi cerdas AI". Dalam hal keamanan komunikasi jaringan, Komunikasi pelanggan di konsol Tencent Cloud dilindungi oleh enkripsi protokol keamanan HTTPS. Layanan VPN Connection juga dapat membantu pelanggan mencapai transmisi yang aman antara pusat data lokal dan sumber daya di Tencent Cloud. Terowongan VPN menggunakan IKE (Internet Key Exchange Protocol) dan IPsec untuk mengenkripsi data yang ditransmisikan, membangun saluran data yang aman dan terpercaya di Internet, sehingga menjaga keamanan data selama perjalanan transmisi. Dalam hal pengendalian dan pengelolaan keamanan jaringan, Tencent Cloud secara internal telah membangun standar manajemen keamanan jaringan dan sistem pertahanan berlapis jaringan. Melalui kebijakan dan prosedur manajemen, Tencent Cloud menetapkan standar kontrol dan perlindungan keamanan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			jaringan serta peran dan tanggung jawab yang sesuai, guna memastikan operasi yang aman dari layanan yang dijalankan di atas jaringan Tencent Cloud. Secara bersamaan, Tencent Cloud menerapkan arsitektur keamanan jaringan yang matang, yang meliputi mekanisme perlindungan berlapis seperti firewall, sistem deteksi/pencegahan intrusi (IDS/IPS), perlindungan DDoS, isolasi logis jaringan, dan keamanan aplikasi web. Mekanisme ini secara aktif mendeteksi, menyaring, dan memblokir lalu lintas jaringan berbahaya untuk melindungi keamanan jaringan Tencent Cloud. Dalam hal manajemen perangkat keras dan perangkat lunak, Tencent Cloud telah menetapkan standar manajemen aset informasi dan proses manajemen siklus hidup lengkap. Hal ini mencakup pengelolaan dan perlindungan aset seperti data elektronik, perangkat keras dan perangkat virtualnya, infrastruktur, sistem aplikasi, serta perangkat lunak melalui klasifikasi dan penilaian tingkat kepentingan. Tencent Cloud mengelola perangkat keras dan komponen perangkat lunak menggunakan sistem manajemen aset, yang meliputi pendaftaran dan pengikatan aset, inventarisasi dan pembaruan informasi aset, serta pensiun dan penggantian aset. Tujuannya adalah untuk memastikan operasi yang stabil dari sistem dasar platform cloud dan memberikan dukungan yang andal bagi sistem

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			bisnis. Tencent Cloud secara berkala pensiunkan dan mengganti server. Komponen perangkat lunak (seperti sistem operasi dan sistem basis data) diganti dengan versi yang sesuai sebelum dukungan berakhir. Untuk hard disk yang telah pensiunkan, Tencent Cloud menerapkan metode penghancuran fisik yang aman untuk memastikan hard disk hancur sepenuhnya, dan mencatatnya dalam catatan penghancuran.
2.g	Pengendalian Akses	g. Bank menerapkan manajemen perlindungan terhadap akses dan pengguna untuk mencegah tindakan tidak terotorisasi pada perangkat, infrastruktur jaringan, dan komponen sistem yang dikelola oleh Bank.	Pelanggan harus membangun mekanisme autentikasi identitas dan kontrol akses untuk data serta sistem teknologi informasi guna mengelola akses ke aset informasi, secara berkala meninjau dan memperbarui izin, serta meningkatkan manajemen keamanan akun pengguna dengan hak istimewa. Dalam hal manajemen akun pengguna dan otorisasi, Cloud Access Management (CAM) membantu pelanggan mengelola akses ke produk dan sumber daya Tencent Cloud dengan aman dan terperinci. Pengguna dapat memodifikasi aturan kata sandi untuk sub-pengguna melalui konsol manajemen akses, termasuk kompleksitas, panjang, dan masa berlaku kata sandi. Untuk mencegah kebocoran kata sandi, Tencent Cloud menggunakan enkripsi SHA256 Hash dan penambahan Salt pada kata sandi pelanggan, sehingga menghindari penyimpanan kata sandi

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			dalam bentuk teks biasa. CAM juga mendukung berbagai metode verifikasi identitas dua faktor, termasuk penggunaan perangkat MFA atau kode verifikasi melalui ponsel, untuk mengonfirmasi keamanan identitas dan lingkungan sebelum login dan melakukan operasi sensitif. Tencent Cloud secara internal juga menetapkan kebijakan otorisasi untuk kontrol akses dan mekanisme matriks pemisahan wewenang, yang mewajibkan akun pengguna menggunakan pengidentifikasi unik. Berdasarkan baseline keamanan, kebijakan kata sandi ditetapkan untuk akun karyawan, termasuk panjang kata sandi, kompleksitas, penguncian, dan reset. Untuk perangkat akhir, sistem operasi, aplikasi, dan perangkat jaringan internal, Tencent Cloud mengonfigurasi batas jumlah kegagalan login dan kebijakan waktu habis sesi. Tencent Cloud menggunakan sistem manajemen keamanan Zero Trust untuk mengautentikasi akses karyawan, yang mewajibkan pengguna untuk menyelesaikan autentikasi dua faktor (2FA) melalui sistem tersebut sebelum mengakses sumber daya internal. Tencent Cloud berpegang teguh pada prinsip hak istimewa paling rendah (principle of least privilege), hanya memberikan izin kepada karyawan berdasarkan tanggung jawab pekerjaan dan kebutuhan bisnis. Tinjauan izin secara berkala dilakukan untuk mencegah penyalahgunaan dan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			penyalahgunaan izin. Untuk pengguna dengan hak akses tinggi, pelanggan dapat menggunakan Cloud Access Management (CAM) untuk mengalokasikan izin sumber daya kepada sub-pengguna melalui metode seperti penanda (tag), guna mencapai kontrol akses terperinci terhadap sumber daya cloud. CAM juga mendukung peninjauan dan pelacakan catatan operasi karyawan melalui CloudAudit. Selain itu, Tencent Cloud menyediakan Bastion Host (BH) yang mampu mendukung otorisasi granular berdasarkan dimensi seperti pengguna, aset, akun, dan izin operasi, memastikan bahwa hak akses yang dimiliki pengguna adalah yang minimal diperlukan untuk mengakses aset dan menyelesaikan tugas kerja. Bastion Host juga mendukung fungsi audit operasi, yang mencatat dan menganalisis log operasi pengguna, sehingga memastikan jejak peristiwa keamanan dapat dilacak secara efektif. Tencent Cloud secara internal juga telah menetapkan persyaratan manajemen dan mekanisme otorisasi terkait untuk hak akses khusus. Secara bersamaan, lingkungan produksi Tencent Cloud telah sepenuhnya menerapkan bastion

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			host, yang digunakan untuk mengontrol secara terpusat hak akses akun administrator komponen sistem backend melalui bastion host tersebut. Akses personel operasional internal ke bastion host memerlukan persetujuan otorisasi, dan hanya personel operasional internal Tencent Cloud tertentu yang dapat mengaksesnya. Login ke bastion host memerlukan autentikasi dua faktor.
2.h	Penggunaan Penyedia Layanan TI	h. Bank menerapkan perlindungan yang memadai dalam pelaksanaan kerja sama antara Bank dengan pihak penyedia jasa TI, termasuk dalam penggunaan cloud.	Pelanggan, ketika bekerja sama dengan penyedia layanan TI termasuk menggunakan penyedia layanan cloud, harus menerapkan langkah-langkah perlindungan yang memadai. Tencent Cloud berpegang pada karakteristik terbuka dan berbagi dari layanan komputasi awan, terus meningkatkan kemampuan keamanan platform dan layanan cloud, serta bersama-sama dengan pelanggan membangun sistem perlindungan keamanan yang lebih baik dan lebih lengkap untuk bisnis dan data di cloud. Sebagai penyedia layanan cloud, Tencent Cloud bertanggung jawab atas infrastruktur pusat data dan keamanan platform cloud. Mengingat bahwa ketika pelanggan memilih kategori layanan cloud yang berbeda (seperti layanan IaaS, PaaS, dan SaaS), tingkat kendali atas komponen yang berbeda juga akan bervariasi. Oleh karena itu, Tencent Cloud telah membangun model Tanggung Jawab Bersama untuk Keamanan Cloud berdasarkan kategori layanan cloud yang berbeda. Detail lebih lanjut dapat dilihat di Bab

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			3 panduan ini: "<u>Model Tanggung Jawab Bersama untuk Keamanan Cloud Tencent</u>". Tencent Cloud merencanakan dan membangun layanan cloud sesuai dengan standar keamanan informasi dan kontrol TI yang diakui secara internasional, serta secara ketat mematuhi hukum dan peraturan terkait perlindungan privasi dan keamanan data di yurisdiksi tempat operasi bisnis berlangsung. Tencent Cloud telah memperoleh berbagai sertifikasi kepatuhan keamanan internasional, menyediakan dukungan produk dan layanan cloud yang telah diaudit dan diakui oleh lembaga sertifikasi pihak ketiga yang berwenang bagi pelanggan. Sebagai penyedia layanan cloud, Tencent Cloud menyediakan dokumen hukum secara online di situs web internasionalnya seperti <u>KETENTUAN LAYANAN</u>、<u>General Service Level Agreement</u>、<u>Perjanjian Privasi dan Keamanan Data</u>, yang secara jelas mengatur konten layanan dan tingkat layanan yang diberikan Tencent Cloud, perlindungan data pengguna dan kekayaan intelektual, serta tanggung jawab dan kewajiban keamanan antara pelanggan dan Tencent Cloud. Pelanggan juga dapat memilih untuk menandatangani perjanjian offline dengan Tencent Cloud guna merundingkan klausul dan ketentuan dalam perjanjian tersebut.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			Tencent Cloud secara aktif mendukung persyaratan manajemen outsourcing pelanggan, menyediakan bantuan khusus dan berkoordinasi dengan audit atau kegiatan penilaian yang dimulai oleh pelanggan. Tencent Cloud juga menyediakan berbagai tindakan perlindungan keamanan serta produk/layanan cloud terkait untuk memastikan kerahasiaan dan integritas data pelanggan di cloud.
			Pelanggan harus mengadopsi standar pengkodean aman, tinjauan kode sumber, dan langkah-langkah keamanan lainnya untuk mencegah kerentanan atau cacat perangkat lunak.
			<u>Cloud Native Build (CNB)</u> menyediakan rantai alat pengembang lengkap dengan kemampuan seperti hosting kode, pipeline pengembangan berkinerja tinggi, asisten kode AI, dan manajemen artefak. Asisten kode AI-nya adalah fungsi bantuan pemrograman AI yang dirancang khusus oleh Tencent Cloud untuk pengembang, mendukung berbagai bahasa pemrograman utama, serta menyediakan fitur seperti penyelesaian kode, pengujian unit, diagnosis kode, tinjauan cerdas, dan tanya jawab cerdas terkait masalah kode. Tujuannya adalah membantu pengembang meningkatkan kualitas dan efisiensi pengkodean.
2.i	Secure Coding	i. Bank memastikan penerapan secure coding dalam pengembangan sistem dan aplikasi untuk meminimalisasi kerentanan atas sistem dan aplikasi.	Untuk pengkodean aman dan peninjauan kode, Tencent Cloud telah menetapkan standar pengkodean aman yang rinci yang mewajibkan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pengembang internal untuk mematuhi dengan ketat. Pelatihan pemrograman aman juga dilaksanakan untuk meningkatkan kesadaran pengembang terhadap risiko seperti serangan injeksi dan kebocoran data sensitif. Selama proses pengembangan, pengembang harus mempertimbangkan fitur keamanan yang harus dimiliki sistem aplikasi guna meminimalkan kemunculan kerentanan. Skema analisis pemeriksaan keamanan kode internal Tencent Cloud mengintegrasikan berbagai kemampuan seperti Static Application Security Testing (SAST), deteksi komponen sumber terbuka, dan deteksi informasi sensitif. Tim bisnis dapat menggunakan kemampuan pemindaian mandiri melalui pipeline untuk melakukan penilaian keamanan pada kode yang akan digabungkan selama tahap akses kode. Masalah tipikal yang ditemukan selama proses peninjauan kode dicatat dan dikumpulkan ke dalam basis pengetahuan tim bisnis. Standar peninjauan kode terutama mencakup deteksi kerentanan lintas bahasa seperti XSS, injeksi SQL, eksekusi kode, injeksi perintah, kerentanan historis pada komponen sumber terbuka pihak ketiga, serta perlindungan informasi sensitif.
2.j	Patching	j. Bank memastikan pelaksanaan patching berjalan dengan baik serta memastikan keandalan dan kemutakhiran seluruh	Pelanggan harus membangun proses manajemen tambalan (patch management), menerapkan tambalan berdasarkan tingkat keparahan tambalan dan pentingnya sistem TI, untuk memastikan keandalan dan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		komponen perangkat lunak, jaringan komunikasi, database, dan sistem operasi (operating system) Bank.	pembaruan tepat waktu dari semua komponen perangkat lunak, jaringan komunikasi, basis data, serta sistem operasi perbankan. Pelanggan dapat menggunakan <u>Cloud Workload Protection Platform (CWPP)</u> untuk mendeteksi kerentanan perangkat lunak Linux, kerentanan sistem Windows, kerentanan Web-CMS, serta kerentanan aplikasi, memberikan peringatan real time, dan mendapatkan solusi perbaikan kerentanan, sehingga membantu pelanggan merespons risiko kerentanan dengan cepat. <u>Tencent Container Security Service (TCSS)</u> mengintegrasikan sistem tambalan virtual yang dikembangkan oleh Tencent Cloud Security untuk melindungi dari kerentanan nol-hari (zero-day vulnerabilities) yang sering muncul. Layanan ini mampu menangkap dan menganalisis kerentanan, menghasilkan tambalan virtual berdasarkan keahlian Tencent, serta secara otomatis mengaktifkan tambalan virtual di server cloud untuk efektif memblokir perilaku serangan peretas. Selain itu, pelanggan dapat menggunakan <u>Vulnerability Scanning Service (VSS)</u> untuk melakukan pemindaian keamanan berkala, peringatan risiko berkelanjutan, dan deteksi kerentanan terhadap ketersediaan, keamanan, serta kepatuhan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			perangkat jaringan dan layanan aplikasi perusahaan. VSS juga menyediakan rekomendasi perbaikan profesional untuk mengurangi risiko keamanan perusahaan. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud akan mengidentifikasi patch terbaru dan melakukan pengujian keamanan yang memadai terhadap patch tersebut sebelum pemasangan, guna memastikan keamanan patch yang diinstal. Tencent Cloud secara berkala memberitahukan tim bisnis internal untuk melakukan pemutakhiran dan pemasangan patch, serta menggunakan alat deteksi endpoint untuk memindai status pemasangan patch secara berkala. Untuk perangkat yang belum menginstal patch melebihi batas waktu yang ditetapkan, sistem akan secara otomatis menghasilkan tiket peringatan. Secara bersamaan, Tencent Cloud juga membangun mekanisme pemindaian kerentanan internal dan platform pengumpulan kerentanan eksternal untuk melaporkan masalah kerentanan serta ancaman dari dalam dan luar. Tiket kerentanan keamanan dicatat dalam sistem operasi keamanan dan ditugaskan kepada penanggung jawab terkait untuk ditangani dalam waktu yang ditentukan. Selain itu, tim riset keamanan Tencent Cloud mengintegrasikan kemampuan perlindungan kerentanan ke dalam sistem Web Application Firewall

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			(WAF) Tencent Cloud dalam bentuk patch virtual, guna memastikan keamanan menyeluruh platform komputasi awan.
3.a	Dokumentasi Kinerja Dasar	a. Bank memastikan ketersediaan dokumentasi kinerja dasar (baseline performance) atas fungsi kritis Bank dan sistem pendukung, agar setiap penyimpangan dapat dideteksi secara tepat waktu serta aktivitas dan kejadian anomali dapat ditandai untuk ditindaklanjuti.	Pelanggan harus menetapkan standar keamanan untuk perangkat lunak dan keras yang mendukung sistem kritis, menerapkan konfigurasi keamanan, serta membangun proses terkait guna memverifikasi penyimpangan konfigurasi dalam sistem dari standar keamanan yang telah ditetapkan. <u>Cloud Security Center (CSC)</u> menyediakan fungsi pemeriksaan dan penilaian otomatis terhadap risiko konfigurasi produk cloud, membantu pelanggan mengurangi risiko keamanan akibat konfigurasi keamanan yang salah dalam penggunaan produk cloud, serta meningkatkan tingkat keamanan cloud secara keseluruhan. Secara bersamaan, pelanggan dapat menggunakan <u>Config Audit</u> untuk melakukan audit dan tata kelola terpusat terhadap sumber daya cloud. Layanan ini secara berkelanjutan mencatat informasi konfigurasi dan perubahan konfigurasi berbagai sumber daya cloud di berbagai wilayah di bawah akun pelanggan, serta melakukan penilaian kepatuhan berkelanjutan terhadap konfigurasi sumber daya cloud di bawah akun perusahaan berdasarkan aturan praktik terbaik Tencent Cloud dan templat paket kepatuhan. Dengan demikian, layanan ini mengidentifikasi

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			konfigurasi sumber daya yang tidak sesuai, sehingga mencapai pemantauan dan pengelolaan otomatis terhadap sumber daya cloud. Tencent Cloud telah membangun sistem manajemen konfigurasi dan mengelola semua komponen layanan TI serta item konfigurasi secara terpusat melalui database manajemen konfigurasi. Hal ini bertujuan untuk menstandarisasi pengelolaan item konfigurasi (CI) dan hubungan di antara mereka. Jika proses perubahan melibatkan pembaruan konfigurasi, personel operasi akan memperbarui versi dan informasi terkait item konfigurasi ke dalam database manajemen konfigurasi sesuai dengan rencana perubahan setelah perubahan selesai dilakukan. Tencent Cloud secara berkala melakukan inventarisasi aset dan mengaudit database manajemen konfigurasi untuk memastikan keabsahan, akurasi, dan kelengkapan informasi setiap item konfigurasi. Selain itu, Tencent Cloud telah membangun seperangkat standar konfigurasi keamanan jaringan dan standar baseline keamanan, yang bertujuan untuk mengelola konfigurasi keamanan perangkat jaringan, firewall, sistem operasi server host, basis data, serta sistem aplikasi secara terstandarisasi. Tencent Cloud secara terus-menerus menggunakan alat pemindaian untuk mendeteksi penyimpangan konfigurasi sistem operasi, sistem manajemen basis data, dan citra

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			virtual dari standar yang telah ditetapkan. Terhadap penyimpangan yang teridentifikasi, Tencent Cloud secara otomatis menghasilkan tiket keamanan dan mengirimkannya ke tim yang bertanggung jawab untuk diperbaiki secara tepat waktu. Tencent Cloud juga secara berkala meninjau kebijakan keamanan dan pengaturan parameter pada perangkat jaringan seperti router, firewall, dan server jaringan untuk memastikan efektivitas kebijakan dan parameter tersebut.
3.b	Pemantauan Keamanan	b. Bank melakukan pemantauan atas aktivitas mencurigakan serta melakukan pengelolaan dan pengujian terhadap proses dan prosedur deteksi untuk memastikan aktivitas anomali dapat dideteksi secara tepat waktu.	Pelanggan harus membangun kemampuan kesadaran situasi keamanan siber, memantau ancaman yang baru muncul, serta mendeteksi peristiwa tidak normal dan ancaman yang memengaruhi sistem kritis, guna memastikan identifikasi, pencegahan, dan respons yang tepat waktu. Untuk mendukung pelanggan dalam mendeteksi dan menganalisis ancaman, Tencent Cloud menyediakan Threat Intelligence Center (TIX). Sebagai platform layanan intelijen terpadu, TIX menyediakan tiga kemampuan intelijen utama: intelijen dasar, intelijen permukaan serangan, dan intelijen bisnis. Platform ini mendukung fungsi seperti kueri intelijen, analisis dan penilaian IOC, serta manajemen permukaan serangan. Kemampuan ini membantu pelanggan menganalisis dan menilai insiden keamanan dengan lebih

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			efisien, serta menilai risiko paparan aset perusahaan secara lebih komprehensif, sehingga mendukung pembangunan sistem pertahanan keamanan multidimensi yang efektif. TIX membangun jaringan titik kontak intelijen yang lengkap, mengumpulkan dan menganalisis intelijen ancaman dari berbagai sumber seperti komunitas kerentanan, lembaga keamanan, penyedia alat keamanan, media sosial, dan blog keamanan. Platform ini juga terintegrasi dengan algoritma dan daya komputasi cloud untuk menghilangkan alarm palsu, sehingga memastikan keakuratan intelijen. Selain itu, Threat Intelligence Center berfokus pada model layanan SaaS, mendukung berbagai metode pengiriman seperti API berbasis web, SDK, TIP, dan mini-program untuk memenuhi kebutuhan pelanggan yang beragam. Threat Intelligence Center juga dapat diintegrasikan dengan produk perlindungan keamanan yang sudah dimiliki pelanggan, sehingga data intelijen dari cloud dapat dikaitkan untuk meningkatkan efisiensi operasi keamanan dan respons ancaman secara keseluruhan. Berdasarkan dukungan dan pemberdayaan dari Threat Intelligence Center, Tencent Cloud berkomitmen untuk membangun sistem kemampuan keamanan pertahanan proaktif yang mencakup "intelijen - serangan dan pertahanan - manajemen - perencanaan". Dengan mengintegrasikan teknologi seperti

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			intelijen ancaman, kecerdasan buatan, dan big data, Tencent Cloud meningkatkan kemampuan dan efisiensi respons terhadap insiden keamanan. Pusat operasi keamanan 7*24 jam juga telah didirikan, yang berfokus pada deteksi, investigasi, dan respons ancaman, guna mencapai visibilitas, keterlihatan, dan kendali yang jelas atas postur keamanan.
3.c, 3.e	Deteksi Kerentanan	c. Bank melakukan pemantauan atau deteksi secara berkelanjutan terhadap kerentanan untuk memastikan efektivitas upaya perlindungan yang telah diterapkan. e. Bank melakukan analisis terhadap ancaman dan kerentanan dari suatu insiden siber untuk memastikan penanganan insiden secara efektif sehingga dapat mencegah terjadinya gangguan pada layanan dan/atau operasional Bank.	Pelanggan harus melakukan pemantauan atau deteksi kerentanan secara berkelanjutan untuk memastikan efektivitas langkah-langkah perlindungan yang telah diterapkan. Dalam hal pengujian penetrasi, Tencent Cloud menyediakan layanan <u>Penetration Testing Service (PTS)</u> bagi pelanggan. Layanan ini sepenuhnya mensimulasikan teknik serangan dan deteksi kerentanan yang mungkin digunakan oleh peretas, dengan menerapkan metode dan pendekatan yang terkendali serta non-destruktif untuk melakukan pemeriksaan mendalam terhadap keamanan sistem target. Hal ini membantu mengidentifikasi kelemahan dalam target dan perangkat jaringan, memberikan rekomendasi penguatan keamanan untuk meningkatkan keamanan sistem pelanggan, serta mendukung verifikasi setelah perbaikan kerentanan dilakukan. Dalam hal pemindaian kerentanan, pelanggan dapat memilih <u>Vulnerability</u>

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			<u>Scanning Service (VSS)</u> untuk mendeteksi aset jaringan perusahaan dan mengidentifikasi risikonya. Berdasarkan pengalaman keamanan dan intelijen ancaman yang dikumpulkan Tencent selama bertahun-tahun, VSS telah membangun basis aturan kerentanan yang kaya dan komprehensif, serta memiliki kemampuan deteksi kerentanan 0Day/1Day/NDay yang profesional dan efisien. Layanan ini dapat melakukan pemindaian keamanan berkala, peringatan risiko berkelanjutan, dan deteksi kerentanan terhadap ketersediaan, keamanan, serta kepatuhan aset pelanggan, sekaligus memberikan rekomendasi perbaikan yang profesional untuk mengurangi risiko keamanan. VSS juga mendukung integrasi dengan produk cloud seperti Host Security dan Web Application Firewall, mencapai siklus tertutup dari pemantauan risiko hingga penanganan risiko. Tencent Cloud secara berkala menyelenggarakan simulasi latihan pertahanan "Tim Merah vs Tim Biru" untuk melawan serangan siber secara realistis. Tencent Cloud juga membangun platform umpan balik kerentanan eksternal dan meluncurkan "Program Penghargaan Kerentanan" yang mengundang pakar keamanan industri untuk membantu mengidentifikasi kerentanan dan risiko keamanan sistem dari perspektif peretas, sehingga masalah keamanan dapat diperbaiki tepat

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			waktu dan keamanan ekosistem Tencent Cloud tetap terjaga.
3.d	Deteksi Insiden	d. Bank memastikan ketersediaan proses untuk mendeteksi insiden siber secara memadai.	Pelanggan harus melakukan pemantauan terpusat terhadap insiden dan kecelakaan keamanan di lingkungan cloud untuk memastikan bahwa insiden keamanan di lingkungan cloud dapat dideteksi dan ditanggapi secara tepat waktu. Tencent Cloud menyediakan Cloud Log Service (CLS). Sebagai platform layanan log terpadu, CLS menawarkan berbagai layanan mulai dari pengumpulan log, penyimpanan log, hingga pencarian dan analisis log, konsumsi real time, serta pengiriman log. Layanan ini membantu pelanggan menyelesaikan berbagai masalah seperti operasi bisnis, pemantauan keamanan, audit log, dan analisis log. Cloud Security Center (CSC) juga mendukung pengumpulan berbagai data keamanan cloud, seperti data peringatan dari produk keamanan cloud, data perubahan konfigurasi aset cloud, data perilaku operasional pengguna di cloud, serta data log dari beberapa produk cloud. Layanan ini menyediakan platform pencarian dan investigasi terpadu untuk membantu pelanggan mencapai audit dan investigasi log cloud yang komprehensif. Selain itu,

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			Elasticsearch Service (ES) mengumpulkan dan mentransmisikan log real time dari cloud server, kontainer, serta produk cloud lainnya, atau data bisnis yang ada dan yang bertambah, ke kluster ES Tencent Cloud untuk penyimpanan terdistribusi, pencarian, dan analisis data. Untuk mendukung kepatuhan pelanggan terhadap persyaratan regulasi, Tencent Cloud mendirikan Pusat Operasi Keamanan (Security Operations Center) yang berbasis teknologi cloud-native. Pusat ini berfokus pada deteksi ancaman, investigasi, dan respons untuk meningkatkan efisiensi operasi keamanan serta mencapai visibilitas, keterlihatan, dan kendali yang jelas atas postur keamanan seluruh jaringan. Tim terkait menjalankan tugas operasi keamanan profesional 7*24 jam, mampu dengan cepat turun tangan dan menangani peringatan keamanan, menyelesaikan analisis awal, serta menyusun rencana penahanan untuk mencegah serangan atau insiden keamanan. Selain itu, berdasarkan pengalaman bertahun-tahun dalam pemantauan perilaku tidak normal, Tencent Cloud telah membangun basis aturan yang komprehensif, di mana aktivitas tidak normal akan secara otomatis memicu peringatan real time. Tencent Cloud juga menetapkan "batas merah" keamanan operasional yang rinci dan secara berkala melakukan tinjauan keamanan operasional internal.

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
4a-f	Proses Penanggulangan dan Pemulihan Insiden Siber	a. Bank menetapkan rencana penanggulangan dan pemulihan insiden siber untuk memastikan penanggulangan dan pengembalian layanan yang tepat waktu sesuai dengan risiko yang ditimbulkan, dengan dampak minimal.	Pelanggan harus menyusun Rencana Respons dan Pemulihan Insiden Keamanan Siber yang mencakup definisi jelas mengenai peran dan tanggung jawab tim respons insiden keamanan siber. Saat insiden terjadi, prosedur pemulihan harus segera dijalankan untuk meminimalkan dampaknya. Pelanggan juga perlu menetapkan saluran komunikasi formal untuk pelaporan insiden keamanan siber, baik secara internal maupun kepada pihak terkait. Selain itu, pelanggan wajib melakukan analisis pasca-insiden dan evaluasi menyeluruh guna memverifikasi keakuratan respons yang diberikan dan efektivitas langkah-langkah yang diambil, serta mendokumentasikan pembelajaran untuk perbaikan berkelanjutan dalam strategi keamanan siber.
		b. Bank menetapkan peran serta tugas dan tanggung jawab tim tanggap insiden siber untuk memastikan penanggulangan dan pemulihan insiden siber dilaksanakan dengan dampak minimal terhadap layanan dan operasional Bank.	Untuk mendukung pelanggan dalam mendeteksi insiden dan merespons dengan cepat, Tencent Cloud menyediakan platform manajemen keamanan terpadu Cloud Security Center (CSC) . Melalui fungsionalitas seperti Pusat Aset, Pusat Risiko, Pusat Peringatan, dan Manajemen Keamanan Tingkat Lanjut, CSC membantu pelanggan mencapai siklus operasi keamanan yang mencakup deteksi ancaman sebelum insiden, respons dan penanganan selama insiden, serta analisis forensik pasca-insiden, sehingga meningkatkan efisiensi operasi keamanan.
		c. Bank menerapkan prosedur pemulihan dan upaya untuk mencegah penyebaran dampak dari suatu insiden siber dengan memitigasi dampak dan menanggulangi insiden siber tersebut.	
		d. Bank melakukan analisis untuk memastikan langkah penanggulangan dan pemulihan insiden siber dijalankan dengan tepat.	
		e. Bank melakukan	

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
		eskalasi dan pelaporan atas insiden siber sesuai dengan jalur komunikasi yang telah ditetapkan. f. Bank melakukan analisis pascainsiden sebagai bahan pelajaran terpetik (lesson learned) dalam penanggulangan dan pemulihan insiden siber untuk perbaikan berkelanjutan.	Dalam hal manajemen insiden, Tencent Cloud telah menetapkan prosedur internal untuk mengelola insiden dan permintaan layanan, serta membangun kebijakan manajemen insiden Tencent Cloud. Hal ini memastikan bahwa insiden terkait aktivitas manajemen layanan TI dicatat dan diklasifikasikan, diprioritaskan berdasarkan tingkat dampak dan urgensi, serta ditingkatkan (escalated) sesuai kebutuhan. Tujuannya adalah untuk menyelesaikan dan menutup berbagai jenis insiden dengan cepat, meminimalkan dampak insiden, menjaga kelancaran operasional bisnis, serta meningkatkan kepuasan pelanggan. Dalam hal komunikasi dan pemberitahuan insiden, Tencent Cloud telah menetapkan standar manajemen insiden keamanan informasi dan membangun prosedur terkait seperti respons insiden keamanan informasi, eskalasi insiden, serta pemberitahuan insiden. Hal ini bertujuan untuk memberikan peringatan atau pemberitahuan tepat waktu kepada pihak internal perusahaan, pelanggan, dan pemangku kepentingan lainnya yang mungkin atau telah terkena dampak insiden, sehingga memastikan semua pihak dapat berkomunikasi dan berkoordinasi secara tertib, cepat, dan efisien. Untuk insiden keamanan yang berpotensi memengaruhi

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			pelanggan, Tencent Cloud akan menilai cakupan dan tingkat dampak insiden keamanan informasi, kemudian setelah melalui tinjauan internal, hasil penanganan dan analisis insiden tersebut akan disampaikan kepada pelanggan melalui saluran yang sesuai. Dukungan teknis juga akan disediakan untuk membantu pelanggan mengambil langkah perbaikan guna meminimalkan kerugian. Dalam hal ringkasan insiden dan peningkatan berkelanjutan, Tencent Cloud telah membangun mekanisme analisis insiden berkala yang melakukan analisis multidimensi terhadap insiden (jenis insiden, frekuensi kejadian, cakupan dampak, dan tingkat keparahan) secara teratur. Berdasarkan tinjauan ulang insiden dan analisis akar penyebab, langkah-langkah pencegahan diambil untuk mencegah terulangnya insiden serupa. Untuk insiden keamanan besar, Tencent Cloud akan membentuk tim khusus untuk menyusun laporan analisis khusus yang disampaikan kepada manajemen. Dalam hal pelanggan melaporkan masalah atau menghubungi Tencent Cloud secara aktif, konsol resmi Tencent Cloud menyediakan layanan tiket yang mendukung pelanggan untuk melaporkan gangguan, insiden, masalah, dan

Nomor	Domain Kontrol	Ringkasan Persyaratan Kontrol	Respons Tencent Cloud
			keluhan terkait keamanan, ketersediaan, dan kerahasiaan. Sistem tiket Tencent Cloud akan mengalokasikan prioritas untuk tiket pelanggan melalui mekanisme respons berjenjang. Ketika tim teknis lini pertama tidak dapat menyelesaikan masalah secara efektif, sistem secara otomatis akan memicu proses peningkatan layanan, di mana tim produk atau tim teknis akan turun tangan untuk menangani secara kolaboratif, guna memastikan kebutuhan atau umpan balik pelanggan mendapatkan respons dan penanganan yang tepat waktu. Tencent Cloud menyediakan layanan pelanggan online dan saluran telepon melalui konsol cloud serta situs web resminya untuk mendukung pelanggan dalam memberikan umpan balik terkait masalah yang dihadapi saat menggunakan layanan Tencent Cloud. Tencent Cloud memiliki pusat layanan pelanggan dengan cadangan lintas wilayah yang mampu menangani permintaan pelanggan secara non-stop 7*24 jam, menyediakan dukungan teknis sepanjang waktu untuk produk cloud, serta respons dan penanganan layanan yang tepat waktu dan berkualitas tinggi. Pelanggan juga dapat memilih paket layanan yang sesuai untuk mendapatkan dukungan eksklusif yang terdiri dari grup dukungan khusus, manajer layanan teknis khusus, layanan bernilai tambah, dan komponen lainnya.

08

Penutup

Tencent Cloud adalah merek komputasi awan yang dibangun dengan dedikasi oleh Tencent Group, mewarisi akumulasi teknologi dan kemampuan praktik keamanan Tencent selama bertahun-tahun. Tencent Cloud berkomitmen untuk terus menyediakan awan yang aman, terpercaya, dan cerdas bagi pelanggan, membantu lebih banyak perusahaan menyambut gelombang digital dengan efisien, serta mendorong perkembangan bisnis yang aman.

Panduan ini didasarkan pada persyaratan regulasi penting dari Otoritas Jasa Keuangan Indonesia, yang secara komprehensif dan transparan menunjukkan kepada pelanggan bagaimana Tencent Cloud dapat membantu mereka mencapai kepatuhan sistem dan data di awan, serta mendukung klien perusahaan dengan percaya diri dan tenang menempatkan sistem dan data mereka di awan. Tencent Cloud berharap melalui panduan ini dapat mendukung klien perusahaan dalam memenuhi standar kepatuhan Otoritas Jasa Keuangan Indonesia secara efektif, sekaligus mencapai peningkatan digital dan inovasi bisnis secara efisien.

Panduan ini hanya sebagai referensi. Untuk informasi dalam panduan ini, pelanggan dapat menggunakannya sesuai dengan kondisi aktual mereka sendiri guna memastikan kepatuhan regulasi selama menggunakan layanan awan Tencent Cloud.

09 Riwayat Versi

Tanggal	Versi	Detail
April 2016	V1.0	Rilis Perdana