腾讯云香港 C-RAF2.0 遵从性指南

2026 年 4 月

CONTENTS

CONTENTS

01 概述

为加强香港认可机构[1]应对网络安全风险的能力，香港金融管理局（Hong Kong Monetary Authority，以下简称“金管局”或“HKMA”）于 2016 年 12 月制定了网络防卫计划（Cybersecurity Fortification Initiative, CFI），其中包括网络防卫评估框架（Cyber Resilience Assessment Framework, C-RAF）、专业发展计划（Professional Development Programme, PDP），以及网络情报共享平台（Cyber Intelligence Sharing Platform, CISP）这三大支柱。2020 年，基于对认可机构的一轮 C-RAF 评估，以及网络安全领域的国际最新发展，金管局对 CFI 进行了全面和独立的审查，并于 2020 年 11 月发布了网络防卫评估框架 2.0（C-RAF 2.0）。

C-RAF 2.0 是一个结构化的评估框架，利用一套控制原则来评估认可机构的固有风险，及其网络安全措施的成熟度，使认可机构能够更好地理解、评估和加强其网络韧性。根据 C-RAF 2.0，认可机构应根据固有风险评级来确定预期的网络安全成熟度级别，然后实施成熟度评估以了解实际的成熟度水平，并识别和改进差距，增强网络韧性。C-RAF 2.0 中规定的评估范围包括支持认可机构香港业务和运营的系统、基础设施、流程和人员。金管局要求认可机构应至少每三年进行一次评估，并应基于认可机构自身的固有风险评级、业务性质的变化或采用的技术等因素，主动考虑更频繁的评估。

腾讯云关注香港金管局的最新监管动态，致力于协助香港金融机构客户满足金管局监管要求。本文将针对 C-RAF 2.0 的网络安全成熟度评估，阐明腾讯云如何协助客户遵从相关的监管要求。

[1] 认可机构：指金管局根据《银行业条例》规定认可的银行、有限制牌照的银行或接受存款的公司。

02

腾讯云安全与隐私合规

合规性是腾讯云发展的基础，腾讯云识别并采用了先进的国际和行业安全标准，遵从不同国家/地区和行业的合规性要求，不断完善内部管理体系，提升腾讯云的安全管控水平，全力打造值得客户信赖的云服务。同时，腾讯云还积极参与行业安全标准的制定及推广，坚持合规即服务，建设和运营安全可靠的云生态环境。

截至目前，腾讯云已通过第三方独立审计或评估的方式，获取多项安全及隐私合规认证或资质，证明腾讯云的安全管理与隐私保护建设满足相关认证标准或行业良好实践，如需了解更多腾讯云合规信息，请参见腾讯云合规性页面。如果需要任何相关的合规证书或报告，请通过腾讯云合规文档中心申请并下载。

腾讯云部分国际权威认证、区域与行业认可示例如下：

2.1 国际权威认证

CSA STAR 云安全认证	STAR 云安全评估是由国际权威的非盈利组织云安全联盟（Cloud Security Alliance）推出的、针对云安全特性的一项国际性认证。它将 ISO/IEC 27001 信息安全管理体系进行拓展，结合云安全控制矩阵（Cloud Control Matrix, CCM），将云安全的特有问题可视化，为用户提供了直观的安全架构评估总览。 基于腾讯公司多年积累的安全实践，腾讯云获得 CSA STAR 全球金牌云安全认证，展示了腾讯云的安全管控体系满足国际权威云安全标准。
SOC 审计	系统与组织控制 报告（System and Organization Controls Reports，下文简称“SOC 报告”）是由专业的第三方会计师事务所依据美国注册会计师协会（AICPA）的相关准则出具的服务机构内部控制相关的系列报告。SOC 报告作为独立的审计报告，涵盖腾讯云平台的安全性，可用性与保密性相关控制点。 根据不同的鉴证服务类型，SOC 报告可提供给云用户以及其审计师，为腾讯云用户提供有价值的信息以供云用户评估和解决与服务机构相关的风险。

2.2 ISO/IEC 体系认证

ISO/IEC 22301: 2019 认证	ISO/IEC 22301: 2019 是以业务连续管理（Business Continuity Management，简称 BCM）为主题的国际标准，提供了一种完整通用的 BCM 方法论，旨在帮助企业识别和应对潜在的破坏性事件，确保关键运营的连续性，从而降低风险并保护组织免受重大影响。

	腾讯云已获得 ISO/IEC 22301: 2019 认证，证明腾讯云已构建了正式的业务连续性管理流程，保障自身业务的连续与稳定。
ISO/IEC 27001: 2022 认证	ISO/IEC 27001: 2022 信息安全管理体系是国际上针对信息安全领域最权威、严格，也是最被广泛接受及应用的体系认证标准。通过该认证，就意味着企业已经建立了一套科学有效的信息安全管理体系，以统一企业发展战略与信息安全管理的步伐，确保相应的信息安全风险受到适当的控制与正确的应对。 通过 ISO 27001: 2022 认证可以更好地体现腾讯云对安全的承诺，表明腾讯云已经建立了科学有效的管理体系，能够为用户提供安全、可靠的云产品和服务。
ISO/IEC 20000-1: 2018 认证	ISO/IEC 20000-1: 2018 是针对 IT 服务管理制定的一套国际标准。该体系规范了企业的信息技术服务管理，从建立、实施、运作、监控、评审、维护与改进的模式，协助企业持续地识别与管理相关信息技术问题，强化与用户的沟通，建立一套自我完善的标准化服务体系。 腾讯云已获得 ISO/IEC 20000-1: 2018 认证，包含云计算服务、托管服务及灾备服务等方面的认证范围。腾讯云严格以服务至上的态度，完善与客户之间的信息技术服务与沟通的机制。
ISO/IEC 9001: 2015 认证	ISO/IEC 9001: 2015 是受国际广泛认可的、成熟的质量管理体系。该体系围绕企业产品或服务提供全过程的质量管理框架和指导性的规范，用于协助企业维持产品或服务，确保交付质量稳定、一致。 腾讯云已获得 ISO/IEC 9001 认证，范围涵盖云计算服务、托管服务及灾备服务等。腾讯云通过使用质量管理体系，有效且高效地实现预期的质量目标，保障云产品和服务的质量和运营。
ISO/IEC 27017: 2015 认证	ISO/IEC 27017: 2015 是 ISO/IEC 27002: 2013 的补充，是云服务信息安全的实用标准，为云服务提供商和客户提供特定安全控制及其实施指南，加强了云计算漏洞的威胁和风险的控制。 腾讯云已获得 ISO/IEC 27017: 2015 认证，不仅表明腾讯云会始终采用国际公认的最佳实践，也证明腾讯云建立了更全面的云安全管理体系，提升了整体云安全服务能力。
ISO/IEC 27018: 2014 认证	ISO/IEC27018: 2014 是针对个人可识别信息（PII）在公共云环境中处理的全球公认的最全面的安全标准。该标准旨在为云服务提供商提供一套保护用户隐私的实践准则，确保在云计算环境下个人数据的安全。

	腾讯云获得 ISO/IEC 27018: 2014 认证，标志着腾讯云个人信息管理系统符合国际严格的个人信息保护法律法规的规定，为腾讯云客户提供了对其云安全的更多信任和保障。
ISO/IEC 29151: 2017 认证	ISO/IEC 29151 是用于实施有关个人身份信息 （PII） 处理的控制措施的国际标准，以满足与 PII 保护相关的风险和隐私影响评估确定的要求。 腾讯云已获得 ISO/IEC 29151: 2017 认证，表明腾讯云基于其 PII 目标和业务需求开发出合适的安全控制体系，为云端的用户 PII 提供高水平的隐私保护控制。
ISO/IEC 27701: 2019 认证	ISO/IEC 27701: 2019 作为 ISO/IEC 27001 和 ISO/IEC 27002 在隐私信息管理的扩展要求和指南，为建立、实施、维护和持续改进隐私信息管理体系提供了指南，是持续管理隐私风险的一个里程碑。 腾讯云获得 ISO/IEC 27701: 2019 认证，证明了腾讯云始终将用户隐私保护作为服务的核心，充分说明了腾讯云产品隐私保护的标准化和可靠性。

2.3 区域与行业认证

德国 C5	云计算合规性标准目录（Cloud Computing Compliance Criteria Catalogue，简称 C5）由德国联邦信息安全局（BSI）制定，旨在基于标准化的检查和报告验证云服务提供商的信息安全合规性。C5 是云服务领域备受行业认可的高级别安全标准。 腾讯云通过了德国 C5：2020 基础和附加审核标准，意味着腾讯云在数据保护和信息安全方面达到了德国政府设定的高标准。
德国 TISAX	TISAX 是德国汽车工业联合会（VDA）联合欧洲汽车工业安全数据交换协会（ENX）推出的汽车行业信息安全评估和数据交换安全标准，TISAX 使得汽车行业内的信息安全评估能够相互认可，并提供了通用的评估和交流机制。 目前腾讯云的多家互联网数据中心（IDC）（包括位于北京、深圳等地）已通过 TISAX 三级评估审核，意味着部署在该区域中的服务均符合 TISAX 的要求，且建立和维护了完善的信息安全管理体系。
新加坡 MTCS T3 认证	新加坡多层云安全（MTCS）标准在新加坡资讯通信发展管理局（IDA）信息技术标准委员会（ITSC）的指导下拟定。MTCS 作为云的常用标准，云服务提供商可采用该标准来解决客户对云端数据的安全性和机密性，以及使用云服务对业务的影响的顾虑。

	腾讯云成功获得了新加坡多层云安全（MTCS）T3 级别标准的认证。此认证意味着腾讯云采取了健全的风险管理机制，以保障云端客户数据的安全性、机密性和可验证的操作透明度。
新加坡 OSPAR	外包服务提供商审计报告（OSPAR）是新加坡金融行业外包服务的准入标准。该标准以新加坡 SSAE 3000 为基础，旨在向新加坡金融机构的服务商在实体层面控制、一般信息技术控制和服务控制三个领域的相关控制设计和操作有效性进行验证。 腾讯云多个产品和服务已经通过了新加坡 OSPAR 审计，并一直努力确保其控制符合 ABS 的指导方针。通过该审计表明腾讯云的安全能力符合新加坡甚至东南亚对金融服务的严格要求。
DPTM 新加坡数据保护信任标记	新加坡数据保护信任标志（DPTM）由新加坡个人数据保护委员会（PDPC）和信息通信媒体发展局（IMDA）制定，旨在为组织展示负责任的数据保护实践。 腾讯云已获得新加坡数据保护信任标志（DPTM）认证，表明腾讯云向客户、业务合作伙伴和监管机构采用了负责任的数据保护实践，有能力保护其收集的个人数据。
新加坡 Cyber Trust Mark	Cyber Trust Mark 是新加坡网络安全局 CSA 推出的国家级网络安全认证，CTM 框架采用基于风险的方法论，评估涵盖 4 个关键领域的 22 个领域组织：治理与风险管理、网络安全运营、韧性、供应链和人员安全以及持续改进与领先实践。 腾讯云已获得新加坡网络安全局颁发的最高级别（Tier 5）网络信任标志。该认证彰显了腾讯云在网络安全治理、风险管理和运营韧性方面的先进能力，使其成为亚太地区受监管和高需求行业值得信赖的云服务提供商。
韩国 KISMS 认证	韩国信息安全保护管理体系（K-ISMS）认证是韩国政府支持的信息安全认证，旨在帮助韩国企业和组织根据适用的韩国信息和通信技术法律始终如一地安全地保护其信息资产。 腾讯云获得 KISMS 认证意味着，韩国的云上客户更易证明其遵守了本地法律要求，从而保护关键数字信息资产，也意味着腾讯云信息安全应对措施和威胁应对程序的能力得到进一步提升，能更加有效地减少安全漏洞的影响。
马来西亚金融行业 IT 合规遵从性审计	马来西亚国家银行（BNM）、马来西亚证券委员会（SC）等马来西亚金融监管机构，颁布了针对金融服务行业的相关法规条例，以规范信息科技在马来西亚银行、保险、证券等金融服务中的应用，保证金融信息系统的可靠性、安全性、稳定性。

	腾讯云通过独立第三方审计可证明，腾讯云在马来西亚为金融客户提供的云服务严格遵守了马来西亚金融行业的监管要求。
香港金融行业 IT 合规遵从性审计	香港特别行政区金融管理局 (HKMA)、证券及期货事务监察委员会 (SFC) 和保险业监管局（HKIA）发布多项关键监管要求，以规范金融、保险和证券机构在信息科技方面的应用。 腾讯云通过独立第三方审计证明，腾讯云是金融行业值得信赖的云服务提供商，腾讯云采取了积极主动的方法履行其最严格的合规义务，金融机构可以放心地基于腾讯云构建其下一代金融服务。
泰国金融行业 IT 合规遵从性审计	泰国金融行业机构需遵守泰国央行（BoT）、 证券交易委员会办公室（OSEC）、保险委员会办公室 （OIC）等金融监管和相关法定机构所颁布的相关法规条例，其监管要求涵盖：信息技术运用中的风险管理、个人信息保护、信息技术在银行、保险、电子政务系统等系统、电子货币、支付系统基础设施、支付服务提供商等中的应用和安全控制等。 腾讯云通过独立第三方审计可证明，腾讯云遵守泰国严格的金融行业监管要求的能力，以及腾讯云致力于为泰国金融行业客户提供优质合规的云服务。
印度尼西亚金融行业 IT 合规遵从性审计	印度尼西亚中央银行 (Bank Indonesia)、金融服务管理局 (Otoritas Jasa Keuangan，OJK) 等印尼金融监管机构，颁布了针对金融服务行业的相关法规条例，其监管要求涵盖了信息技术运用中的风险管理、个人信息保护、信息技术在银行、保险、电子政务系统等系统、电子货币、支付系统基础设施、支付服务提供商等中的应用和安全控制。 腾讯云通过了由独立第三方审计机构执行的印度尼西亚金融合规性审计，证明腾讯云在印尼为金融客户提供的云服务严格遵守了印尼金融行业的监管要求。
菲律宾金融行业 IT 合规遵从性审计	菲律宾金融行业机构需遵守菲律宾中央银行（BSP）等金融监管和相关法定机构制定的相关法规条例，其监管要求涵盖了信息技术运用中的风险管理、个人信息保护、信息技术在银行、保险、电子政务系统等系统、电子货币、支付系统基础设施、支付服务提供商等中的应用和安全控制。 腾讯云通过独立第三方审计，可证明腾讯云遵守菲律宾严格的金融行业监管要求的能力，以及致力于为金融行业客户提供优质合规的云服务。
美国电影协会 MPAA	美国电影协会（MPAA）建立了一套安全存储、处理和传递受保护的媒体内容的最佳实践标准。本实施指南旨在让与 MPAA 协会成员保持合作关系的应用程序和云服务供应商了解在内容安全方面应遵循的要求。MPAA 内

	容安全模板的组件参照了相关的 ISO 标准（27001-27002)、安全标准（即 NIST、CSA、ISACA 及 SANS）和行业最佳实践。 腾讯云已获得 ISO 27001、ISO 27017、ISO 27018、PCI DSS 以及 CSA STAR 等相关认证。且腾讯云已通过自评估的方式，确保其对客户内容的管理程序遵守美国电影协会（MPAA）内容安全模型指南。
美国 HIPAA	美国《HIPAA 法案》的目的之一是推动电子健康记录的使用，通过加强信息共享来提高医疗系统的效率和质量。HIPAA 关注及保障实体及其商业伙伴在创建、接收、维护和传输等环节中，受保护的健康信息（Protected Health Information，PHI）的安全性（包括可用性、完整性和保密性）和隐私性。受 HIPAA 监管的实体及其商业伙伴需要在处理、维护和存储 PHI 等场景中提供相应的安全措施。 腾讯云通过自评估的方式，确保腾讯云对于用户个人信息的安全保护能力及控制措施的有效性遵从了 HIPAA 的合规要求。
美国 SEC Rule 17a-4	腾讯云对象存储服务（COS）根据美国证券交易委员会（SEC）、金融业监管局（FINRA）和商品期货交易委员会（CFTC）的技术要求，由专门从事记录管理和信息治理的独立第三方评估公司进行认证。 该认证为在高度监管环境（例如金融服务行业）中运营的客户保证了腾讯 COS 的不可重写、不可擦除的保存方法和对象锁定功能，展示了腾讯云致力于为客户提供安全、符合行业标准的云产品的承诺。
日本 FISC	为了提高金融机构的安全性，《FISC 银行及相关金融机构计算机系统安全指南》为日本银行和金融机构建设安全的信息系统、保障信息系统的运行提供了有效指导。 腾讯云依据该指南对控制现状进行了评估，以确认腾讯云的相关措施满足 FISC 银行及相关金融机构计算机系统安全指南的要求。
英国 BS10012: 2017	BS10012: 2017 由英国标准协会发布，旨在为组织提供隐私保护的合规框架和良好实践，指导企业建立和维护个人信息管理体系（PIMS），确保组织拥有充分和适当的控制措施来保护个人信息。该体系已更新和修订以符合《通用数据保护条例》。 腾讯云已获得 BS10012: 2017 认证，体现了腾讯云的个人信息管理体系满足国际标准和行业良好实践的要求，使客户能够更好地遵守 GDPR 的隐私保护要求。

欧盟 CISPE	CISPE 行为准则是根据欧盟《通用数据保护条例》（GDPR）第 40 条针对云基础设施服务提供商的泛欧行业特定准则，帮助欧洲各地的组织加速为消费者、企业和机构开发符合 GDPR 的基于云的服务。 腾讯云已授予 CISPE 行为准则“候选”标志，这意味着腾讯云已根据 CISPE 行为准则要求完成了自我评估，用于证明腾讯云在文档体系和实施层面的合规性。
NIST CSF 认证	NIST CSF 是一个框架，侧重于使用业务驱动因素来指导网络安全活动，并将网络安全风险视为组织风险管理流程的一部分，帮助组织根据其业务需求、风险承受能力和资源调整其网络安全活动并确定其优先级，并且组织可以通过应用该框架的风险管理原则和指南来提高安全性和韧性。 腾讯云已获得由第三方机构认证的 NIST CSF 认证，不仅是对腾讯云网络安全防御体系能力的肯定，也表明腾讯云能够有效识别、抵御、应对和处置安全风险，保护客户的云资产和数据，增强了客户对腾讯云安全稳定的信心。
PCI DSS 认证	支付卡行业数据安全标准（PCI DSS）由支付卡行业安全标准委员会（PCI SSC）创建和维护。为增强持卡人的数据安全，PCI DSS 针对保护账户数据的技术和操作要求提供了全球统一的基准，适用范围涵盖所有涉及支付卡处理的实体，像商户、处理商、收单机构、发卡机构和服务提供商，以及储存、处理或传输持卡人数据的其他实体。 腾讯云已经通过 PCI DSS 认证审核，获得 PCI DSS 1 级服务提供商资质。证明腾讯云在可为客户提供安全可靠的支付服务，保护持卡人的数据安全。
GxP 合规性	在医疗保健行业，GxP 涵盖了广泛的合规相关活动，它通常是指一套规范药品、医疗器械和医疗软件应用程序等医疗产品的开发、制造和销售的法规、指南或行业良好实践。 腾讯云发布了 GxP 合规白皮书，向医疗行业的客户阐述腾讯云的管理流程和技术措施可帮助客户满足 GxP 计算机化系统的要求；以及确保腾讯云对于托管在腾讯云上的客户业务数据的机密性、完整性和可用性。

03

腾讯云安全责任共担模型

当前越来越多的客户在选择云计算服务提供商及其提供的产品与服务时，将安全作为首要考虑的因素之一。

腾讯云秉持云计算服务的开放、共享特性，持续提升云平台和云服务的安全能力，并与客户一起为云端业务和数据构建更好更完善的安全保障体系。腾讯云作为云服务提供商，负责数据中心的基础设施和云平台的安全。考虑到当客户选择不同的云服务类别（例如 IaaS、PaaS 和 SaaS 服务）时，对不同组件的控制权也会有所不同，为此腾讯云基于不同的云服务类别建立了云安全责任共担模型。其中定义浅蓝色部分由腾讯云负责，浅灰色部分为客户负责，浅绿色部分则表示腾讯云和客户将共同承担相应的责任。

	IaaS	PaaS	SaaS	
客户的责任	云客户的数据安全	云客户的数据安全	云客户的数据安全	
	云客户的账号和访问控制策略	云客户的账号和访问控制策略	云客户的账号和访问控制策略	
	云上安全配置策略	云上安全配置策略	云上安全配置策略	不同服务场景的共担责任
	云上应用安全	云上应用安全	云上应用安全	
	云上虚拟化网络和主机安全	云上虚拟化网络和主机安全	云上虚拟化网络和主机安全	腾讯云的责任
	云平台和产品自身安全合规	云平台和产品自身安全合规	云平台和产品自身安全合规	
	物理和基础架构安全	物理和基础架构安全	物理和基础架构安全	

图 1 腾讯云信息安全责任共担模型

腾讯云对上图中不同安全属性的解释如下：

- 云客户的数据安全：指客户在云计算环境中的业务数据自身的安全管理，包括上传、存储、分发、加工及其他方式处理的客户业务数据等方面。
- 云客户的账号和访问控制策略：指客户注册的腾讯云账号信息，以及基于云账号下的所有授权行为，包括账号信息、密码、访问控制策略、身份验证等信息。
- 云上安全配置策略：指为正确开发或使用云产品（含安全产品），基于不同场景与业务安全要求匹配的安全产品和安全配置策略。

- 云上应用安全：指在云计算环境下的业务相关应用系统的安全管理，包括应用的设计、开发、发布、运维、监测运营等。
- 云上虚拟化网络和主机安全：指云计算环境下的主机和网络安全管理，其中网络层面包括虚拟网络、负载均衡、安全网关、VPN、专线链路等方面；主机层面包括云计算、云存储、 云数据库等云产品的底层管理（如虚拟化控制层、数据库管理系统、磁盘阵列网络等）和使用管理（如虚拟主机、镜像、CDN、文件系统等）。
- 云平台及云产品自身安全合规：指云计算环境下的云平台及所提供的云产品/服务自身的安全和合规。
- 物理和基础架构安全：指云计算环境下的数据中心安全运营、物理服务器和物理网络设备的安全管理等。

有关安全责任共担模型的更多信息请参阅《腾讯云安全白皮书》。

04

腾讯云全球基础设施

腾讯云在全球范围内布局了多个数据中心，形成了一个庞大的基础设施网络，能够为全球客户提供快速稳定、智能可靠的就近服务。腾讯云在中国大陆、亚太地区、北美地区、欧洲地区已开放 20+个地理区域（Region），运营 60+个可用区（Availability Zone），为更多企业提供强有力的技术支持，助力业务飞速拓展，帮助客户灵活应对不同地区的法规要求，满足金融行业企业对数据本地化存储和业务全球化的需求，确保数据处理的合规性、安全性与高效性。

- 地域（Region）是指物理的数据中心的地理区域。腾讯云不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议客户选择最靠近的地域。
- 可用区（Zone）是指腾讯云在同一地域内电力和网络互相独立的物理数据中心。其目标是能够保证可用区间故障相互隔离（大型灾害或者大型电力故障除外），不出现故障扩散，使得用户的业务持续在线服务。通过启动独立可用区内的实例，用户可以保护应用程序不受单一位置故障的影响。

腾讯云目前在中国境内部署 2300+加速节点，覆盖多运营商，境外布局 900+加速节点，覆盖全球 70+国家地区，通过将服务内容分发至全网加速节点，利用全球调度系统使用户能够在就近节点获取所需内容，降低访问延迟。

腾讯云还通过设立独立站点，以及采用数据加密、访问控制、审计追踪等技术手段，增强数据的隔离性和安全性，防止数据泄露和非法访问，强化数据的地域性隔离与合规性处理。

关于腾讯云基础设施的更多信息，请参阅腾讯云全球基础设施页面。

05

腾讯云如何遵从及协助客户满足《C-RAF 2.0》

《C-RAF 2.0》的网络安全成熟度矩阵为认可机构提供了不同成熟度级别应符合的控制目标和控制原则，覆盖治理、识别、保护、检测、响应与恢复、态势感知、第三方风险管理这七个领域。

在本章节中，腾讯云将提炼和总结《C-RAF 2.0》中针对认可机构在基线（Baseline）、中级（Intermediate）、高级（Advanced）这三种不同成熟度级别下的控制要求，以便客户参考进行合规建设，并阐述腾讯云作为云服务提供商，如何协助认可机构遵从相关要求。

5.1 领域一：治理

5.1.1 战略与政策

编号	控制域	控制要求总结	腾讯云的应答
1.2.1	战略与计划	基线：认可机构应制定网络安全战略以及自上而下的行动计划，以提升网络安全水平。 中：除上述控制外，认可机构还应明确提升网络韧性的方向与措施，并与其业务发展方向、采用的新技术以及安全行业标准等相衔接。 高：除上述控制外，认可机构还应对网络安全战略进行定期的审查更新，并制定短期和长期的发展计划。	在网络安全战略方面，为应对数字化时代下更复杂的网络威胁和安全风险，腾讯发布了“数字安全免疫力”模型框架，提出用免疫的思维应对新时期下安全建设与企业发展的协同关系，以企业数据和业务为目标，建设韧性、自适应、可扩展的安全免疫体系，为企业在数字时代的高质量发展保驾护航。 腾讯云以“加强企业数字安全免疫力，助力数字时代下的韧性发展”为目标，致力于完善其云安全体系、建设安全合规能力、制定云安全标准。基于全面规划的模型框架，通过多元化的产品与安全属性，腾讯云实现了全方位的防护，并在各个层面的产品中实现了对应的安全功能。 此外，腾讯云会定期评审其安全方针/战略，并根据业务情况、技术发展等按需更新。
1.2.2	政策	基线：认可机构应制定经董事会或专门委员会网络安全相关政策，以管理网络风险与韧性。 中：除上述控制外，认可机构还应根据固有风险状况的变化，定期对网络安全政策进行审查和更新。 高：除上述控制外，认可机构还应对各业务线涉及的网络风险相关政策进行交叉引用，并及时更新。	腾讯云制定了信息安全管理政策，由信息安全总体战略、安全组织架构及安全管理体系组成，有效支撑云平台的安全运行与风险管理。腾讯云信息安全政策每年定期进行评审，确定云安全管理体系的控制目标、控制程序和控制措施符合相关安全策略、标准、程序和法律要求，确保信息安全政策的充分性和有效性。员工可以通过内部平台查看腾讯云发布的这些政策。

5.1.2 人员配备与培训

编号	控制域	控制要求总结	腾讯云的应答
1.5.1	人员配备	基线：认可机构应识别和明确定义网络安全相关的角色与职责，承担网络安全职责的员工需具备相关的能力和资质。 中：除上述控制外，认可机构还应明确具备网络安全知识和经验的人员负责网络安全相关工作。对应聘人员、承包商以及第三方人员开展相应的背景调查。 高：除上述控制外，认可机构还应针对网络安全相关的岗位制定人才发展方案，聘用专职的网络安全人员参与和制定网络安全防御战略。	腾讯设立了安全技术委员会和不同职能、不同领域的专业安全团队，并在内部建立了完善的人力资源管理标准及程序，确保根据岗位要求招聘和安排人员。在招聘过程中，腾讯云会对备选雇员进行审查，包括验证学历、资质证书等。腾讯云集结了行业资深的专家服务团队，致力于为客户提供安全、可靠、专业的安全合规产品和服务。此外，腾讯云还设置了多元化的职业发展路径，为员工配备了丰富且高质量的学习资源，持续优化培训课程和体系，以支持员工的个人成长和职业发展。
1.5.2	培训	基线：认可机构应定期为员工开展网络安全与技能提升培训，对不同角色和岗位的人员提供其职责相关的网络安全培训。 中：除上述控制外，认可机构还应在员工岗位发生变动时或基于风险的方法识别出意识薄弱的员工时，开展特定的网络安全培训。 高：除上述控制外，认可机构还应针对管理层、安全人员、全体员工等制定不同的培训计划和培训内容。认可机构也应与安全行业机构和团体就建立联系，获取最新的安全实践动态。	腾讯云内部建立了完善的信息安全培训机制，要求正式员工、顾问、实习生和外包员工等学习信息安全培训课程。腾讯云提供了多样化的培训课程，包括全员必修培训、重点岗位专项培训和自选专业课培训等，内容覆盖基础安全意识、办公安全、漏洞识别与防御、隐私保护、应急响应、研发安全规范和数据安全要求等方面。

5.2 领域二：识别

5.2.1 IT 资产管理

编号	控制域	控制要求总结	腾讯云的应答
2.1.1	IT 资产管理	基线：认可机构应建立准确和完整的操作环境视图，从而全面掌握整体攻击面。 中：除上述控制外，认可机构应建立流程对信息系统的安装、移除和更新保留记录并更新资产清单。 高：除上述控制外，认可机构还应部署工具和/或流程，可用于对 IT 资产清单的跟踪、更新、资产优先级划分，并可用于检测和阻断对软硬件的未经授权的变更。	为协助客户进行全面的信息资产管理，腾讯云提供了**主机安全（CWPP）**，支持自动化采集资产指纹，并统一管理账号、端口、进程、应用等资产指纹数据。CWPP 还能够基于资产指纹对已发生的安全事件风险影响面进行快速调查，以帮助客户提高服务器安全。客户还可采用腾讯云一站式安全管理平台**云安全中心（CSC）**来进行信息资产安全管理。CSC 涵盖资产安全中心功能，能够帮助客户实现对云上资产的自动化动态盘点，包括云服务器、对象存储、云数据库、负载均衡等，并通过云配置风险、漏洞及安全事件等多种安全维度对资产安全风险进行统一管理，降低云上“影子 IT”风险。 为配合客户遵从控制原则，腾讯云制定了信息资产管理规范和全生命周期管理流程，对电子数据、硬件及其虚拟设备、基础设施、应用系统和软件等资产进行分类分级管理和保护。腾讯云通过资产管理系统对硬件设备及软件组件进行管理，包括资产登记及绑定、资产盘点及信息更新、资产退役及更换等等，保障云平台底层系统平稳运行，为业务系统提供可靠的支撑。

5.3 领域三：保护

5.3.1 访问控制

编号	控制域	控制要求总结	腾讯云的应答
3.1.1	用户账号管理	基线：应建立针对系统、应用程序和硬件的身份验证与访问控制机制，并实施权限管理与审计、密码策略与密码加密、生产与非生产环境隔离等防止未经授权访问的措施。 中：除上述控制外，应建立用户权限变更的监控告警机制，以及密码生成和修改时与常用密码库进行校验的机制。	**访问管理（CAM）**能够帮助客户安全且精细化地管理对于腾讯云产品和资源的访问。其中用户主账号默认拥有其名下资源的完全访问权限，可以创建子用户并为子用户分配身份 ID、身份凭证和权限。用户可以通过访问管理控制台修改子用户的密码规则，包括密码的复杂度、长度、有效期等信息。为防止密码泄露，腾讯云会对客户密码采用 SHA256 哈希（Hash）加密和加盐（Salt）

编号	控制域	控制要求总结	腾讯云的应答
		高：除上述控制外，应建立针对协作计算设备和应用程序的访问控制机制（如适用），并对非特权账户的本地访问实施多因素身份验证。	处理，避免存放密码明文。CAM 还支持通过操作审计（CloudAudit）查看和跟踪员工的操作记录。 为配合客户遵从监管要求，腾讯云内部制定了访问控制管理规范，要求用户账号使用唯一标识符，并根据安全基线为员工账号设置密码策略，包括密码长度、复杂度、锁定和重置等。腾讯云通过零信任安全管理系统对员工进行准入认证，用户访问内部资源需要先完成双因素身份验证。 腾讯云内部也制定了授权策略和权限分离矩阵机制，遵循最小权限原则，根据岗位职责分配所需操作权限，并对权限设置有效期限，实现权限的精细化管控。腾讯云会维护岗位角色对应人员身份信息与各业务系统权限级别的记录，并通过定期组织内部权限审核工作，确保权限不会被滥用、误用。 此外，腾讯云制定了严格的内部网络隔离规则，通过物理和逻辑隔离的方式实现了腾讯云内部办公网络和客户数据所在的生产环境的完全隔离。腾讯云还为生产环境全面部署堡垒机，以防止未经授权的访问。
3.1.2	特权用户账号管理	基线：应建立严格的特权用户管理机制，并对特权账户实施多因素身份验证。 中：除上述控制外，应建立特权用户的访问控制及审计审查机制，为信息系统执行最小特权原则，并将多因素身份验证用于高风险系统。 高：除上述控制外，应限制网络访问的特定特权命令的使用，并记录要求此类访问的理由。	访问管理（CAM）通过精细化权限管控、操作审计，以及多种方式的二次身份校验等功能，能够为客户的特权账号管理提供帮助。 腾讯云还提供堡垒机（BH），能够支持基于用户、资产、账号、操作权限等维度进行细粒度授权，确保用户所拥有的权限是其访问资产、完成工作任务的最小化权限。堡垒机支持操作审计功能，对用户的操作日志进行记录和分析，确保安全事件有效追溯。 为配合客户遵从监管要求，腾讯云内部明确了特殊访问权限的管理要求和相关授权机制。同时，腾讯云生产环境已全面部署堡垒机，通过堡垒机对腾讯云后端系统组件的管理员账号权限进行集中管控。内部运维人员访问堡垒机需要经过授权批准，仅特定的腾

编号	控制域	控制要求总结	腾讯云的应答
			讯云内部运维人员可以访问，登录堡垒机需要双因素身份验证。运维操作记录由日志平台集中存储，由腾讯云内部审计团队定期对日志进行审核。
3.1.4	物理访问管理	应为 IT 硬件、通信系统实施控制，限制和记录针对高风险或机密系统的物理访问。对物理访问进行监控和告警，并定期审查物理访问日志。	**在物理安全方面**，腾讯云依据数据中心相关的国际标准和监管要求，建立了一套全方位的数据中心安全管理体系，并定期进行严格的内外部审计，通过持续改进以保证云计算数据中心的物理和环境安全，致力于为每一位客户提供安全、稳定、持续、可靠的物理设施基础。腾讯云在全球的数据中心均按照相关国际标准和当地安全要求进行选址、建设或租赁。 **在安保与监控方面**，腾讯云各数据中心的安保人员严格根据巡检清单和巡检计划对各机房和设备情况进行巡检，并在每个检查点签名和记录检查时间，一旦发现基础设施故障或安全事件，会立即启动数据中心紧急事件响应流程。同时，腾讯云为数据中心配备了 7*24 小时无盲点的视频监控告警系统，由保安室值守，且监控记录安全存储并保留充足时间。 **在物理访问控制方面**，腾讯云各数据中心根据不同级别的区域安全要求制订了严格的访问控制策略。各类访客或工作人员出入数据中心均需进行身份核对和随身物品检查，并登记携带物品。腾讯云根据人员类别和访问权限，在数据中心门禁授权系统建立了完整的人员访问控制安全矩阵，实现对数据中心各类人员访问、操作等行为的有效管控。此外，腾讯云金融专区的物理机房还通过专用围笼将不同客户的设备进行物理隔离，并配备生物识别门禁系统，能够有效防止非授权人员接触客户的设备。

编号	控制域	控制要求总结	腾讯云的应答
3.1.5	远程访问管理	基线：应对员工、承包商和第三方的远程访问使用加密连接和多因素身份验证，并为具有网络访问权限的非特权账户实施多因素身份验证。 中：除上述控制外，应实施加密机制来保护远程访问会话的机密性和完整性，并通过集中管理的网络访问控制点路由所有远程访问，以监控远程访问会话和审计用户活动。 高：除上述控制外，应按需授权和记录通过远程访问方式的特权命令执行或安全相关信息访问，相关记录应定期审查，且应具备快速断开或禁用对信息系统的远程访问的能力。	为了便于客户在任何时间、任何地点、使用任何主流终端，安全、快速地接入云端业务系统，腾讯云支持 SSL VPN 远程访问技术。SSL VPN 可以通过加密方式保护在互联网上传输的数据安全性，也支持进行适当的访问控制，减少非授权访问情况的发生。 客户还可以使用 **VPN 连接（VPN Connection）** 实现本地数据中心与腾讯云上资源连通的传输。VPN 通道采用 IKE（密钥交换协议）和 IPsec 对传输的数据进行加密，在 Internet 上建立一条安全、可信的数据隧道，保障传输途中数据安全。VPN 网关具有高可靠性，底层采用双机热备架构，保障通信会话不中断，上层应用无感知。 腾讯云内部建立了员工远程访问管理相关程序，员工仅能使用已在腾讯云上注册的可信设备，并通过加密通信通道远程访问腾讯云办公网和日常办公系统。腾讯云会维护远程访问日志，记录用户操作行为。 腾讯云内部办公网络和客户数据所在生产环境完全隔离，当腾讯云员工获得客户的同意与授权访问客户信息资产时，必须通过双因素认证经堡垒机访问客户数据所在的生产环境。腾讯云在权限授予时采用细粒度权限划分，仅授予员工提供服务所需要的最小运维权限和时限。后台运维操作记录均由日志平台集中存储，由腾讯云内部审计团队定期对记录信息进行审核。
3.1.8	加密密钥管理	应制定涵盖密钥生成、分发、安装、更新、撤销和到期的加密密钥管理策略和程，并采取控制措施，防止未经授权访问加密密钥。	腾讯云提供了**密钥管理系统（KMS）**以协助客户实现针对加密密钥的全生命周期管理，确保密钥以安全的方式完成生成、存储、分发、导入、导出、使用、恢复、归档与销毁等一系列操作，防止密钥被泄露。KMS 使用 FIPS-140-2 认证的硬件安全模块（HSM）来生成和保护密钥，并能够支持客户加密密钥的全生命周期管理。为减少密钥被破解或滥用的风险，KMS 支持密钥轮换，并采用安

编号	控制域	控制要求总结	腾讯云的应答
			全可靠的方法删除失效、作废或泄露的密钥。删除后的密钥将无法恢复，此密钥下的加密数据也将无法解密。 腾讯云内部建立了密钥管理机制，制定相关标准，规范密钥的申请、生成、存储、使用、传递、更新、销毁等过程。涉及密钥生命周期的各项操作均执行双重控制、严密交接、妥善保管、及时更新的基本要求，建立并履行权责分离、指定责任人，严格审批、详细记录、实名操作的规章制度，并保留业务密钥操作日志，定期进行操作审计。

5.3.2 基础设施保护控制

编号	控制域	控制要求总结	腾讯云的应答
3.2.1	网络保护	基线：应设置网络边界防护措施防止未经授权的网络连接，包括边界防御工具、入侵检测/防御系统（IDS/IPS）、对高风险网络端口的持续监控、在互联网接入点以及 DMZ 区与内网之间部署防火墙、防火墙规则变更审批和定期审计机制等。 中：除上述控制外，应将企业网络分区，采用深度防御策略，对所有管理控制台的远程访问实施安全控制，采取反欺骗措施来检测和阻止伪造的源 IP 地址进入网络，以降低网络攻击风险。 高：除上述控制外，应部署工具和/或制定流程阻止不安全的员工自有设备或未经授权设备的访问，限制和监控可信与不可信网络区域之间的流量，并定期或按需评估和审查网络安全架构、配置及流程，识别差距并补救。	**为实施网络边界防护**，腾讯云为客户提供了**边缘安全加速平台（EO）**，基于腾讯全球边缘节点向客户提供安全防护和加速服务，具有 DDoS 防护、智能 Web 防护、BOT/爬虫类攻击防护、DNS 解析等功能，并支持客户根据业务需求配置自定义访问控制规则。客户还可选用云防火墙、Web 应用防火墙，以及 DDoS 防护（Anti-DDoS）等网络边界防护工具。**云防火墙（CFW）**主要提供不同网络边界的防护，支持防火墙 ACL 主动管控、IPS 实时拦截、虚拟补丁和恶意代码检测等功能，可实现传统网络中的 DMZ 区需求，将核心资产重点防护，实现 VPC 间的细粒度隔离管控。**Web 应用防火墙（WAF）**能够应对 Web 攻击、入侵、漏洞利用、挂马、篡改、后门、爬虫等网站及 Web 业务安全防护问题。**DDoS 防护（Anti-DDoS）**通过充足、优质的 DDoS 防护资源，结合持续进化的“自研+AI 智能识别”清洗算法，应对 DDoS 攻击问题。

编号	控制域	控制要求总结	腾讯云的应答
			针对网络分区要求，客户可以使用腾讯云提供的**私有网络（VPC）**服务为其已购买的云平台资源构建多个独立的网络空间，并自定义网段划分和 IP 地址、自定义路由策略等。VPC 服务是基于腾讯云构建的专属云上网络空间，私有网络基于隧道技术，在物理网络上构造虚拟网络，使用虚拟化技术，实现不同私有网络之间内网完全隔离，为客户提供独立、隔离的安全云网络。对于私有网络内的云服务器，可通过配置安全组及网络 ACL 规则，实现对实例级别及子网的出入流量的控制，达到不同层面的网络访问控制。 **在网络流量监控方面**，客户可选用**网络流日志（FL）**，对网络流量进行实时、非侵入的旁路采集、存储和分析，以解决故障排查、架构优化、安全检测以及合规审计等问题。 **在网络通信安全方面**，客户在腾讯云控制台上的通信受到了 HTTPS 安全协议的加密保护。为了便于客户在任何时间、任何地点、使用任何主流终端，安全、快速地接入云端业务系统，腾讯云支持 SSL VPN 远程访问技术。SSL VPN 可以通过加密方式保护在互联网上传输的数据安全性，也支持进行适当的访问控制，减少非授权访问情况的发生。 此外，客户还可以使用**云联网（CCN）**实现云上私有网络间（VPC）、VPC 与本地数据中心间（IDC）的安全内网互联。 **针对腾讯云内部的网络安全防护与管理，腾讯云建立了网络安全管理规范和网络纵深防御体系。**腾讯云通过管理制度和流程明确了网络安全管控和防护标准，以及对应的角色和职责，确保腾讯云网络承载的业务得以安全运行。同时，腾讯云参考业界实践设计网络安全架构，根据业务功能和安全风险进

编号	控制域	控制要求总结	腾讯云的应答
			行安全域划分，对不同安全域进行物理或逻辑隔离，通过访问控制和边界防护等措施确保办公网络、开发网络、测试网络、生产网络的安全。腾讯云通过防火墙、入侵检测/防御系统（IDS/IPS）、DDoS 防护、Web 安全防护等多重防护机制，及时检测、过滤并阻止恶意网络流量，保护腾讯云的网络安全。 此外，腾讯云部署了内部网络监控系统对路由器、防火墙和网络服务器等网络设备进行监控和告警，并通过权限管控、审批流程等多重措施，严禁非授权人员访问内部网络资源。 **在防火墙的使用与管控方面**，腾讯云的防火 墙规则被配置为限制对腾讯云生产网络的访问。对防火墙规则的管理访问仅限于使用安全外壳（“SSH”）协议和双因素身份验证的授权管理人员，且防火墙规则的更改在部署前会通过相关的审查和批准流程。腾讯云定期对防火墙规则进行全面审计，重点核查规则的使用情况。
3.2.2	系统配置	基线：应建立和实施系统配置管理，包括根据行业标准设置应用系统/网络设备/操作系统安全配置基线，管控系统配置变更，限制覆盖系统、对象、网络、虚拟机和应用程序的控制程序的使用，限制软件安装，预设置系统会话管理，以及禁用不必要的端口、功能、协议和服务。 中：除上述控制外，应定期审查关键系统，以识别潜在的漏洞、升级机会或新的防御层，并对不受支持的系统实施控制，且定期测试相关控制。 高：除上述控制外，应采取控制措施防止设备或系统组件执行未经授权的代码，并主动识别可能被用于零日攻击的控制漏洞。	腾讯云为客户提供了**主机安全（CWPP）**，基 于腾讯积累的海量威胁数据，帮助客户管理基线安全。CWPP 支持基线检测，包括一键检测、定期检测等可选模式，并支持查看基线通过率和修复建议。CWPP 还提供腾讯云默认基线策略，进一步助力客户的服务器基 线安全。腾讯云还提供了**云安全中心 （CSC）**，支持针对云产品配置风险的自动 化检查评估，覆盖云服务器、对象存储、云数据库及负载均衡等多种云产品，能够帮助客户降低因云产品使用中的错误安全配置带来的安全风险，提升整体云上安全水平。 同时，客户可以通过**配置审计（Config）**实 现对云资源进行集中审计和治理，持续记录客户账号下不同地域的各种云资源的配置信息和配置变更，并基于腾讯云最佳实践的

编号	控制域	控制要求总结	腾讯云的应答
			规则和合规包模板，自动对企业账号下的云资源配置进行持续的合规性评估，识别不合规的资源配置，从而实现对云资源的自动化监控和管理。 为配合客户遵从监管要求，腾讯云内部建立了一套网络安全配置标准和安全基线标准，旨在对网络设备、防火墙、主机服务器操作系统、数据库以及应用系统的安全配置进行标准化管理。腾讯云通过配置扫描工具持续检测操作系统、数据库管理系统和虚拟镜像的配置与标准的偏差。针对识别到的偏差，腾讯云会自动生成安全工单并发送至责任团队，及时修正。腾讯云还会定期对路由器、防火墙和网络服务器等网络设备的安全策略和参数设置进行审阅，确保策略和参数的有效性。 在主机安全层面，腾讯云部署了终端检测与响应（EDR）工具，对全网服务器终端资产进行全面监测和管控。腾讯云采用的 EDR 工具支持防病毒与入侵检测、安全基线与漏洞扫描、以及针对命令操作、登录行为的安全合规审计等功能，并在识别到恶意程序、异常行为时触发监控告警。腾讯云通过工单系统跟进和处理告警事件。
3.2.3	虚拟化安全	应制定策略以管理虚拟机镜像和快照的创建、分发、存储、使用、退役、销毁以及安全，并实施控制措施以限制对管理程序和主机操作系统的管理员模式访问。	腾讯云为客户提供的**云服务器 (CVM)** 是可 扩展的虚拟化计算服务，支持客户自定义 CPU、内存、硬盘、网络、安全等资源。腾讯云向客户提供安全的官方公共镜像，包含官方正版的基础操作系统和腾讯云提供的初始化组件。CVM 还支持客户制作或通过镜像导入功能导入自定义镜像，以及共享和删除自定义镜像。此外，CVM 支持快照功能，包括手动快照及定期快照，以支持数据日常备份、数据快速恢复、快速部署环境等业务场景。 为保障 CVM 安全性，客户可通过安全组和网络 ACL 自定义主机和网络的访问策略，灵活为不同实例设定防火墙。CVM 也已支持敏感操作保护功能，在用户进行敏感操作前对其进行身份验证。腾讯云还为 CVM 提

编号	控制域	控制要求总结	腾讯云的应答
			供云监控，支持多种实时预警，并提供 DDoS 防护、DNS 劫持检测、入侵检测、漏洞扫描、网页木马检测、登录防护等安全服务。 针对容器镜像的管理，**容器镜像服务 (TCR)** 能够为客户提供安全、专用、高性能的容器镜像托管和分发服务。客户也可采用**容器安全服务 (TCSS)** 保护容器及镜像安全。TCSS 支持容器资产管理、镜像安全扫描、运行时入侵检测、安全基线配置管理等功能，能够帮助客户建立容器安全防护体系，从镜像生成、存储到运行，为容器提供全生命周期保护。 **为加强腾讯云虚拟机及虚拟服务使用过程中的安全管控**，腾讯云内部制定了虚拟化安全管理相关规范，明确了虚拟机资源的管理责任、权限管理、配置管理等相关标准。腾讯云通过虚拟机隔离和资源控制、补丁管理和漏洞防护、Hypervisor 安全加固等技术手段，从多方面构建虚拟化安全防御体系。

5.3.3 数据保护

编号	控制域	控制要求总结	腾讯云的应答
3.3.2	数据保护	基线：认可机构应制定相关政策和流程明确数据加密、数据销毁等数据安全相关标准，对通过公共或不受信任的网络传输的机密数据，以及存储机密数据的移动设备进行加密，在合规要求的时间内处置或销毁数据，并对在非生产环境中使用的客户数据进行脱敏。 中：除上述控制外，应采用工具来防止和/或检测未经授权访问或泄漏机密数据。 高：除上述控制外，机密数据在专线	**在数据存储保护方面**，腾讯云多款存储和数据库产品均支持数据加密功能，使用安全的高强度加密算法，并通过集成**密钥管理系统 (KMS)** 实现密钥全生命周期管理，确保数据机密性。**密钥管理系统 (KMS)** 使用 FIPS-140-2 认证的硬件安全模块 (HSM) 来生成和保护密钥，并能够支持客户加密密钥的全生命周期管理。为减少密钥被破解或滥用的风险，KMS 支持密钥轮换，并采用安全可靠

编号	控制域	控制要求总结	腾讯云的应答
		和可信区域内传输时应进行加密。	的方法删除失效、作废或泄露的密钥。删除后的密钥将无法恢复，此密钥下的加密数据也将无法解密。此外，腾讯云在存储数据时采用多副本冗余存储和纠删码技术，在检测到完整性错误时立即采取必要的恢复措施，极大提高了数据的容错能力。 **在数据传输保护方面**，客户在腾讯云控制台上的通信均受到 HTTPS 安全协议的加密保护。腾讯云云产品所提供的云 API 接口亦具有 HTTPS 加密、签名校验、状态监测等安全能力，为客户的业务提供端口级别的通信安全保障。此外，客户还可使用以下腾讯云服务来实现不同场景下的数据安全传输： • **专线接入（DC）**：提供具备专用性与高安全性的大带宽网络连接。用户独占网络链路，无数据泄露风险。 • **VPN 连接 (VPN Connection)**：基于网络隧道技术，实现本地数据中心与腾讯云上资源连通的安全传输。VPN 通道采用 IKE（密钥交换协议）和 IPsec 对传输的数据进行加密，在互联网上建立一条安全、可信的数据隧道，保障传输途中数据安全。 **针对数据的删除与销毁**，腾讯云提供安全可靠的数据销毁机制。当客户的云服务终止后，腾讯云遵循严格的数据擦除方式，在保留期限届满后彻底删除包括副本和备份在内的客户数据，删除后的数据无法复原。当用于提供腾讯云服务的介质出现故障需要更换或者到达使用期限需要报废时，腾讯云会及时遵照严格的流程进行彻底的物理销毁。

5.3.4 安全开发

编号	控制域	控制要求总结	腾讯云的应答
3.4.1	安全开发	基线：认可机构应建立框架及对应流程、程序和控制以管理系统开发生命周期（“SDLC”），确保框架与 DevOps 政策、IT 服务管理流程保持一致，明确敏捷软件开发标准，并将访问控制、身份验证、授权、数据完整性、日志记录、安全事件跟踪和异常处理等安全要求嵌入 SDLC 各阶段中。 中：除上述控制外，应制定并实施各阶段/活动安全标准，建立漏洞管理机制，并在连接互联网的应用程序发布或更新前对其进行安全测试。 高：除上述控制外，应制定并实施严格的变更和发布管理程序，控制 SDLC 各阶段/活动达到安全标准，包括充分审查应用与服务间的依赖关系，发布前对应用进行代码审查和/或静态代码分析，并对应用及 API 进行安全测试。	为支持客户进行研发管理，腾讯云提供了开发者工具**云原生构建（CNB）**。CNB 基于 Docker 生态，对环境、缓存、插件进行抽象，并采用声明式语法，旨在帮助开发者以更高效的方式构建软件。CNB 提供完整的开发者工具链，具备代码托管、高性能研发流水线、AI 代码评审、云上开发环境、制品管理、自定义任务集等能力，能够有效实现从需求到部署的研发全流程支持及敏捷开发管理。 腾讯云内部亦已建立一套信息系统安全开发标准，并着力将 ISO/IEC 20000 信息技术服务管理标准、ISO/IEC27001 信息安全管理体系和 ISO/IEC 9001 质量管理体系标准融入到产品安全开发生命周期全流程中，在产品需求、设计、研发、测试、交付、运维等不同环节，融入信息安全和隐私保护理念，确保云产品在其生命周期内均能获得足够的安全管控。相关安全管控措施包括： • 安全培训：通过安全编程培训培养开发人员的安全编程意识，严格要求相关人员遵循安全编码规范； • 需求分析：针对业务内容、业务流程、技术框架进行沟通，寻找安全嵌入的最优方式； • 系统设计：对系统设计进行威胁建模，对采用的架构进行安全技术评估； • 系统开发：开发过程中，提供腾讯自行设计的安全开发组件供研发人员使用，并依照腾讯云的安全编码规范进行编码； • 安全验证：通过代码安全检查、资产安全扫描、Web 扫描、人工安全测评、渗透测试和代码审计等发现漏洞； • 发布：经过安全部门的最后检查确认后，系统才能发布到线上环境，以防止产品携带安全漏洞在生产环境运行。

5.3.5 补丁和变更管理

编号	控制域	控制要求总结	腾讯云的应答
3.5.1	补丁管理程序	基线：建立正式的补丁管理计划和流程，为系统配置从官方来源检索补丁，确保软件和固件补丁得到及时应用，并对补丁管理报告进行审查。针对识别的安全补丁缺失应制定适当的后续处理流程。 中：除上述控制外，应实施工具和/或流程识别缺失的安全补丁以及每个补丁可用的天数。 高：除上述控制外，应确保补丁监控覆盖所有服务器，并审查补丁管理报告时以确保安全补丁在严格的时间框架内测试和实施。	为配合客户遵从监管要求，在补丁管理方面，腾讯云会识别最新的补丁，并在安装补丁前对补丁进行充分的安全测试，确保安装补丁的安全性。腾讯云会定期通知内部各业务团队进行补丁升级和安装，并使用终端检测工具定期扫描补丁安装情况，并对超期未安装补丁的设备自动生成告警工单。 腾讯云还建立了内外部漏洞识别机制。针对外部漏洞，腾讯云构建以 TSRC（腾讯安全应急响应中心）为核心的协同漏洞奖励计划，通过外部白帽子众测机制覆盖云产品及核心业务系统，结合 AI 驱动的威胁情报分析与多维度验证流程，系统性识别外部脆弱性。针对内部环境，腾讯云使用漏洞扫描系统对云环境中的资产进行定期扫描。识别到的安全漏洞会通过安全工单通知相关部门进行评估和跟进处理，在规定的时间内完成修复和验证。
3.5.2	补丁评估和测试	基线：建立流程和控制措施，应在补丁应用于系统和/或软件之前对其进行测试，尽量减少因补丁引起的兼容性问题。 中：除上述控制外，在部署安全补丁之前，应评估应用安全补丁的影响；还应维护、跟踪、定期审查和及时处理积压的漏洞。 高：除上述控制外，应利用自动化和分类来促进大规模和快速的修补。	
3.5.3	变更管理流程	基线：认可机构应建立变更管理流程，用于申请和审批对 IT 系统配置、硬件、软件、应用程序和安全工具的变更。 中：除上述控制外，应在实施变更期间评估网络安全风险，指派适当人员负责变更审批，并确保所有基线 IT 配置的变更经过审批和安全影响评估。 高：除上述控制外，应明确需要对变更影响进行网络风险评估的阈值或场景，并实施工具以检测和阻止对软/硬件未经授权的更改。	为配合客户遵从监管要求，腾讯云已建立一套关于产品和配置变更的管理标准，明确了变更流程中的各个步骤以及相关的责任人，以确保变更在实施前经过适当的审批和测试。同时，腾讯云定义了紧急变更的管理流程，紧急变更需得到适当的审批后才可进行。 腾讯云的变更发布管理程序覆盖应用程序和配置文件、操作系统及数据库的变更。这些变更在上线前均需进行业务影响分析、独立的功能测试，制定变更的备份与回滚计划，并经相关责任人批准。腾讯云变更发布系统强制要求变更操作只能由授权人员执行，并保留变更相关的日志，定期进行审核。变更发布后，腾讯云运维团队会在生产环境

编号	控制域	控制要求总结	腾讯云的应答
			中对变更情况进行监控并验证变更结果。 此外，针对可能会对客户产生影响的运维变更操作，腾讯云将及时通过官网、站内信等渠道向相关客户发布变更通知。

5.3.6 修复管理

编号	控制域	控制要求总结	腾讯云的应答
3.6.1	修复管理	基线：认可机构应建立修复管理流程，及时修复网络风险评估中识别的问题、渗透/模拟测试中发现的弱点，并通过后续漏洞扫描进行确认。 中：除上述控制外，应重复模拟测试，以确认中高风险可利用漏洞已得到解决。 高：除上述控制外，应建立组织资产维护和维修的审批与授权流程，并记录和审查资产的维护和维修情况。针对已识别的高风险或无法有效解决的问题，应上报管理层处理。	**为协助客户进行漏洞修复和资产风险管理**，腾讯云提供了**云安全中心（CSC）**。云安全中心支持云上资产一站式安全管理，包括资产的自动化盘点、资产各类安全风险的检测与识别，以及资产安全风险的自动化响应处置。依托腾讯的情报能力，云安全中心能够为客户推送当前的最新漏洞并提供详细的漏洞介绍报告，包括漏洞影响面及处置建议等，帮助客户实现对高危漏洞的及时感知和快速处置。云安全中心还利用编排能力支持客户预置自动化处置与响应，以提升威胁响应效率。 **在容器漏洞修复与管理方面**，**容器安全服务（TCSS）**能够定期或及时扫描本地和存储库镜像中的漏洞，实时获取官方来源的漏洞信息，并定期更新漏洞库。容器安全服务支持腾讯云漏洞利用防御系统，基于虚拟补丁防护零日漏洞，能够集成腾讯的漏洞挖掘和实时高危漏洞告警技术以捕获和分析漏洞，并根据腾讯的专业知识生成虚拟补丁，自动在云服务器上生效，有效拦截黑客攻击行为。 **为配合客户遵从监管要求，在漏洞修复管理方面**，腾讯云建立了威胁与脆弱性管理相关程序，以便及时识别和采取措施来改善或修补信息系统面临的威胁和漏洞。腾讯云定期

编号	控制域	控制要求总结	腾讯云的应答
			对信息系统进行漏洞扫描和渗透测试，测试过程中会复核过去遇到的威胁和漏洞，并通过重复执行的测试确认漏洞的修复情况。扫描或测试过程中识别到的安全风险会通过安全工单通知相关部门进行评估和跟进处理。如评估发现漏洞可能对客户业务产生影响，则会通过官网公告、站内信的方式及时将漏洞相关信息通知客户。通知的内容包括但不限于漏洞描述、影响范围及程度、腾讯云已采取的控制措施、为客户提出的修复建议及具体操作指引。 **在软/硬件的维修和维护方面**，腾讯云通过 资产管理系统对硬件设备及软件组件进行管理，包括资产登记及绑定、资产盘点及信息更新、资产退役及更换等。腾讯云定期对服务器进行退役和更换，软件组件（如操作系统和数据库系统）则在支持终止前更换为合适版本。

5.4 领域四：检测

5.4.1 漏洞检测

编号	控制域	控制要求总结	腾讯云的应答
4.1.1	防病毒和反恶意软件	基线：认可机构应部署自动更新的检测攻击和保护设备的防病毒和反恶意软件工具，并对电子邮件采取保护措施过滤常见的网络威胁。 中：除上述控制外，认可机构应实施流程和工具（如沙盒）进行自动行为分析，以检测并阻止恶意软件。 高：除上述控制外，认可机构应制定集中管理及自动更新的端点保护机制。	客户可采用主机安全（CWPP）为云主机提 供安全防护。CWPP 基于积累的海量威胁数据，利用机器学习为客户提供黑客入侵检测、漏洞风险告警等安全防护服务，包括密码破解阻断、异常登录提醒、木马文件检测、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险。 **在物理主机安全层面**，腾讯云部署了终端检 测与响应（EDR）工具，对全网服务器终端资产进行全面监测和管控。腾讯云采用的 EDR 工具支持防病毒与入侵检测、安全基线与漏洞扫描、以及针对命令操作、登录行为的安全合规审计等功能，并在识别到恶意程

编号	控制域	控制要求总结	腾讯云的应答
			序、异常行为时告警。腾讯云通过工单系统跟进和处理告警事件。
4.1.2	渗透/模拟测试	基线：认可机构应根据业务系统和内部网络安全评估的结果进行定期的渗透测试和漏洞扫描。 中：除上述控制外，认可机构应定期或发生重大变更时开展模拟测试。此外，认可机构还应在系统部署到生产环境之前进行渗透和漏扫，并全年覆盖所有生产环境中的高风险系统。 高：除上述控制外，认可机构应制定终端设备的漏洞扫描流程。	**在渗透测试方面**，腾讯云为客户提供渗透测试服务（PTS），通过完全模拟黑客可能使用的攻击技术和漏洞发现技术，采用可控制、非破坏性质的方法和手段对目标系统的安全做深入的探测，发现目标和网络设备中存在的弱点，提供安全加固意见帮助客户提升系统的安全性，并支持漏洞修复后的验证。 **在漏洞扫描方面**，客户可选用漏洞扫描服务（VSS）探测企业网络资产并识别其风险。依托腾讯多年累积的安全经验与威胁情报，VSS 建立了丰富而全面的漏洞规则库，并具备专业高效的 0Day/1Day/NDay 漏洞检测能力，能够对客户资产的可用性、安全性与合规性等进行定期的安全扫描、持续性风险预警和漏洞检测，为客户提供专业的修复建议，降低安全风险。VSS 还支持与主机安全、Web 应用防火墙等云产品进行联动，实现从风险监测到风险处置的闭环。 **为配合客户遵从监管要求，腾讯云内部建立了定期的漏洞扫描与渗透测试机制。**腾讯云内部的漏洞扫描通常包括 web 漏洞、组件漏洞、配置扫描等，通过漏洞扫描系统自动生成扫描任务对云环境中的资产进行漏洞扫描，并对发现的漏洞进行分析、分类和修复处理。在渗透测试方面，腾讯云安全团队定期开展全链路大型渗透测试，并在新产品上线前或重大变更等情况下灵活开展针对性渗透测试。测试结果通过安全工单的形式通知相关责任部门，由责任部门及时进行漏洞修补或实施其他补偿性控制措施，确保渗透测试中发现的可利用漏洞已得到妥善处

编号	控制域	控制要求总结	腾讯云的应答
			理。此外，腾讯云定期开展红蓝对抗模拟抵御网络攻击的实战演练。

5.4.2 异常活动检测

编号	控制域	控制要求总结	腾讯云的应答
4.2.1	日志监测和分析	基线：认可机构应建立日志监控的机制，对物理和逻辑访问、第三方对关键系统的访问、特权账户的活动等进行日志记录和监控，并进行时钟同步。应定期对日志记录和安全实践日志进行审查。 中：除上述控制外，认可机构应将审计日志备份到集中式日志服务器或介质中。 高：N/A	腾讯云为客户提供了日志服务（CLS）以协助进行日志管理。作为一站式日志服务平台，CLS 支持从日志采集、日志存储到日志检索分析、实时消费、日志投递等多项服务，协助客户解决业务运营、安全监控、日志审计、日志分析等问题。腾讯云 CLS 采用高可用的分布式架构设计，对日志数据进行了多冗余备份存储，防止单节点服务宕机数据不可用，提供服务高可用性，为日志数据提供稳定可靠的服务保障。客户还可采用以下云产品辅助进行日志监控与分析： • 云安全中心 (CSC)：能够统一采集云安全产品告警数据、云资产配置变更数据、云上用户操作行为数据及部分云产品日志数据等各类云上安全相关数据，并提供统一检索调查平台，帮助客户实现全面的云上日志审计与检索调查。 • 操作审计 (CloudAudit)：支持对腾讯云账号进行监管、合规性检查、操作审核和风险审核。客户可以借助 CloudAudit 记录日志、持续监控并保留与整个腾讯云基础设施中操作相关的账号活动。 • Elasticsearch Service (ES) 服务，将云服务器、容器等其他云产品实时日志，或业务的存量及增量业务数据，汇聚传输到腾讯云 ES 集群，进行数据的分布式存储、

编号	控制域	控制要求总结	腾讯云的应答
			查询分析。 为配合客户遵从监管要求，腾讯云内部建立了日志收集与管理规范及机制，对登录日志、操作日志、事件日志等日志数据的记录、提取、分析、审计等进行管控，以检测和防范系统活动异常和风险。腾讯云对员工账号的登录状态实施实时安全监控，一旦检测到任何异常登录行为，IT 安全系统将立即联系账号所属人进行核查与处理，并详细记录相关事件。 此外，腾讯云生产环境已全面部署堡垒机，在生产环境中的运维操作均须通过堡垒机进行。运维操作记录由日志平台集中存储。 腾讯云通过运维安全自动化审计工具和内部审计团队对日志进行审计，以防范操作风险。
4.2.2	安全信息和事件管理	基线：认可机构应建立安全事件管理流程以检测异常活动。设定阈值以确定日志中需要进行安全响应的活动。 中：除上述控制外，认可机构应部署用于检测未经授权的数据挖掘工具，主动监控安全日志中的异常行为。 高：除上述控制外，认可机构应建立系统以监控和分析员工行为，并采取措施监控敏感数据或文件。此外，认可机构应采用深度防御技术检测和响应网络安全攻击。	日志服务（CLS）支持对一个或多个日志主题设置告警策略，告警策略会周期性执行监控任务，当查询分析结果满足触发条件时发送告警通知，方便客户及时发现异常问题。 客户还可选用数据安全审计（DSA）来监测针对数据的异常操作。DSA 是一款基于人工智能的数据库安全审计系统，支持对企业网络中的数据库各类会话信息、访问操作、SQL 语句进行全量审计入库，根据多种规则库和威胁检测引擎识别操作中的恶意行为，并及时通知管理员采取相应的安全防护措施。对于已发生的安全事故，数据安全审计也支持对数年的日志进行审计和分析，为企业还原安全事故全貌并定位责任人提供参考依据。 **为配合客户进行安全事件管理**，腾讯云内部制定了信息安全事件管理规范，建立了信息安全报告、响应和处理机制及相关流程，并规范了事件日志的记录与告警机制。腾讯云团队在监测到安全事件或接收到来自其他事件发现者的报告后，会立即启动响应机制，并进行多维度的预警和防御。腾讯云安

编号	控制域	控制要求总结	腾讯云的应答
			全团队依托 7×24 小时安全运营体系，聚焦漏洞监测、入侵溯源、攻击阻断等核心场景，实时响应安全告警并快速完成攻击溯源与应急处置方案制定，有效遏制安全事件扩散。 **在数据防泄漏方面**，腾讯云对数据访问权限 实行了全节点实名制审核和维护，以保障数据资产的完整性和业务服务的可靠性，并建立了实时监控和拦截机制，以检测和阻止任何异常的数据访问行为。此外，腾讯云还对员工个人计算机部署了数据防泄漏（DLP）工具，以有效限制数据导出，并监控、检测与防止潜在的数据盗窃活动。 **在网络攻击防御方面**，腾讯云部署了成熟的 网络安全架构，通过防火墙、入侵检测/防御系统（IDS/IPS）、DDoS 防护、网络逻辑隔离、Web 应用安全等多重防护机制，应对网络威胁。有关腾讯云网络安全及相关产品的 更多信息请参考本指南**第 5.3.2 章节“基础 设施保护控制”**。

5.4.3 网络事件检测

编号	控制域	控制要求总结	腾讯云的应答
4.3.1	事件监控	基线：认可机构应建立事件监控机制，对物理和逻辑环境中的未经授权的行为进行监控，并明确监控和报告异常行为的责任。 中：除上述控制外，认可机构应建立网络活动基线，部署工具以检测未经授权的数据传输，并对关键资产进行监控。 高：除上述控制外，认可机构应制定评估恶意行为的流程和解决方案。	腾讯云可观测平台（TCOP）提供对云产品/云资源的实时监控、分析和告警服务，可收集并通过可视化图表展示腾讯云云产品自助上报的各项监控指标和客户自定义配置上报的监控指标，帮助客户实时掌握云产品运行状况和性能，并支持针对指标设置告警，根据所设置的告警规则，通过消息推送等方式及时将业务异常通知客户。客户还可使用云安全中心（CSC），通过其资产中心、风险中心、告警中心、高级安全管理功能，实现事前威胁检测、事中响应处置、事后溯源分析的安全运营闭环。云安全中心支持周期性检测端口风险、漏洞风险、弱口令风险、内容风险、云资源配置风险和服务暴露六大风险，持续监测企业安全情况，并统一接入云防火墙、Web 应用防火墙、主机安全的日志数据，对告警日志进行审计、分析、聚合、统一展示和跟踪。 为配合客户遵从监管要求，腾讯云设置了内部网络监控系统对路由器、防火墙和网络服务器等网络设备进行监控和告警，并部署了终端检测与响应（EDR）工具，对全网服务器终端资产进行全面监测和管控。腾讯云采用的 EDR 工具支持防病毒与入侵检测、安全基线与漏洞扫描、以及针对命令操作、登录行为的安全合规审计等功能，并在识别到恶意程序、异常行为时触发告警。腾讯云通过工单系统跟进和解决识别到的安全问题。 同时，腾讯云设定了详细的运维安全“红线”，并凭借在异常行为监控方面多年累积的经验建立了完善的规则库，打造了可靠的运维安全自动化审计工具，可以及时识别异常行为和自动触发实时告警。
4.3.2	检测与告警	基线：认可机构应建立事件检测和告警机制，使用多来源的工具和流程来检测、告警和触发事件响应机制。 中：除上述控制外，认可机构应通过自动化流程实时检测事件，实现持续的检测和响应。 高：除上述控制外，认可机构应使用自动化工具来检测对关键系统文件和安全设备的未经授权的更改，部署网络监控和检测工具，并关联多个事件来源。	

5.4.4 威胁监测和分析

编号	控制域	控制要求总结	腾讯云的应答
4.4.1	威胁监测和分析	基线：认可机构应建立威胁情报收集、监控与分析的机制。 中：除上述控制外，认可机构应明确威胁情报监控与分析的职责，并建立安全运营中心，7*24 对系统进行持续的监控。 高：除上述控制外，认可机构应对威胁情报进行分析，明确风险细节及应对威胁的缓解措施。利用多来源的威胁情报，更新组织的 IT 安全架构和 IT 配置标准。	为支持客户进行威胁检测与分析，腾讯向客户提供了**威胁情报中心（TIX）**。作为一站式情报服务平台，威胁情报中心可提供基础情报、攻击面情报、业务情报三大情报能力，支持情报查询、IOC 研判分析、攻击面管理等功能，能够协助客户更高效地对安全事件进行分析研判，和更全面地评估企业资产暴露面的风险情况，助力企业构建高效的立体化安全防御体系。威胁情报中心构建了完整的情报触点网，从漏洞社区、安全机构、安全工具厂商、社交媒体、安全博客等多种来源收集和分析威胁情报，并联动云端算法算力去除误报，保障了情报的准确性。 此外，威胁情报中心以 SaaS 化为核心，支持 Web 端 API、SDK、TIP、小程序等多种交付方式，满足不同客户需求。威胁情报中心还可以通过被集成方式，将云端情报数据与客户现有的安全防护产品进行联动，以提高整体安全运营和威胁响应效率。 基于威胁情报中心的赋能与支持，腾讯云致力于构建“情报-攻防-管理-规划”的主动防御安全能力体系，通过整合威胁情报、人工智能、大数据等技术，提升安全事件的响应能力和效率，并设立了 7×24 小时安全运营中心，聚焦威胁检测、调查和响应，实现安全态势的可知、可见、可控。

5.5 领域五：响应与恢复

5.5.1 事件响应与恢复的治理与准备

编号	控制域	控制要求总结	腾讯云的应答
5.1.1	事件响应与恢复的治理	基线：认可机构应明确界定各相关利益相关方在网络事件响应与恢复中的责任与职责分工，确保相关方能够及时参与应对。 中：除上述控制外，认可机构应开展	**为保证客户业务的持续可用**，腾讯云为云产品和关键流程制定了详细的容灾恢复预案，并严格按照要求进行定期演练确保容灾恢复预案的及时性与可行性。

编号	控制域	控制要求总结	腾讯云的应答
		对可能在事件发生期间或之后为其提供协助的技术来源、咨询公司或取证服务机构的尽职调查，应与事件响应组织或服务提供商建立直接的合作或合同协议，应建立严格的变更管理流程以审查和批准访问权限变更。 高：除上述控制外，认可机构应制定全企业范围内可操作且协调一致的计划，确保网络事件响应与恢复方法融入各业务部门的灾难恢复计划、业务连续性计划和危机管理计划。	**在事件的响应与处置方面**，腾讯云内部制定了信息安全事件管理规范，建立了信息安全报告、响应和处理机制及相关流程，并使用内部安全运营系统记录安全事件。针对检测识别到的安全事件，腾讯云会结合事件性质、数据敏感程度和影响范围等因素，对安全事件进行分析和分级，并及时知会相应的责任人跟进处理事件。 腾讯云还建立了网络安全应急预案，覆盖网络攻击、恶意程序、数据安全、设备设施故障、灾害性事件等多类网络安全应急场景，以建立健全应急预案体系为基础，以建设应急处置队伍为支撑，以规范应急处置流程为重点，进一步增强监测预警、通报处置等工作能力，预防和减少网络安全事件对腾讯云的不利影响。
5.1.2	事件响应与恢复的准备	基线：认可机构应建立针对网络事件响应与恢复的计划和应对手册，明确启动相关措施的标准，涵盖业务影响分析、业务连续性计划、灾难恢复计划、危机管理计划以及数据备份方案。 中：除上述控制外，认可机构应制定相关计划，以确保在启动应急预案时能够迅速恢复核心任务和业务功能。还需要制定明确的恢复目标，包括恢复点目标（RPO）和恢复时间目标（RTO），确保在发生网络事件时能够迅速恢复关键业务功能。 高：认可机构应部署多个系统和方案，定期进行测试和演练，确保在发生网络事件导致能力或服务受损时能够迅速响应并恢复关键业务，以实时或接近实时的方式进行恢复和维护，并将运营损失降至最低。	**在业务连续性管理与灾难恢复方面**，腾讯云已获得 ISO/IEC 22301 业务连续性管理体系的国际标准认证。腾讯云构建了全面的业务连续性管理体系，规范了业务连续性管理相关流程，覆盖业务影响分析、业务连续性计划、应急响应和灾难恢复、应急演练与测试、危机管理等方面。腾讯云也明确了灾难事故期间的内/外部通讯策略，并建立了联系人清单。腾讯云每年根据业务影响分析的结果审查其灾难恢复计划，并按需更新。 此外，作为云服务提供商，腾讯云会积极配合客户的外包管理要求，包括根据客户实际的需求提供和签署相关服务协议、积极响应及配合客户方发起的评估或调查活动等。

5.5.2 分析、缓解与恢复

编号	控制域	控制要求总结	腾讯云的应答
5.2.1	分析	基线：认可机构应识别网络安全事件，对事件进行严重性的分级评估。 中：除上述控制外，认可机构应在入侵事件发生之前，提前进行安全事件分析。 高：除上述控制外，认可机构应关联和整合威胁情报、网络运维和事件响应，并制定事件响应与恢复目标。在适当条件下，引入第三方参与安全事件演练。	为配合客户遵从控制原则要求，腾讯云内部制定了信息安全事件管理规范，建立了信息安全报告、响应和处理机制及相关流程。腾讯云使用内部安全运营系统记录安全事件。针对检测识别到的安全事件，腾讯云会结合事件性质、数据敏感程度和影响范围等因素，对安全事件进行分析和分级，并及时知会相应的责任人跟进处理事件。 同时，腾讯致力于构建“情报-攻防-管理-规划”的主动防御安全能力体系，通过整合威胁情报、人工智能、大数据等技术，提升安全事件的响应能力和效率。腾讯云安全团队依托 7×24 小时安全运营体系，聚焦漏洞监测、入侵溯源、攻击阻断等核心场景，实时响应安全告警并快速完成攻击溯源与应急处置方案制定，有效遏制安全事件扩散。 对于可能影响到客户的安全事件，腾讯云会根据信息安全事件的影响范围和程度，在经过内部评审后，将信息安全事件的处理和分析结果通过合适的方式通知客户。 在适当的情况下，腾讯云也可为客户的安全事件演练提供相关的技术支持。
5.2.2	缓解	基线：认可机构应建立最小化解决网络事件造成影响的策略和流程，涵盖第三方发生的网络安全事件。 中：除上述控制外，认可机构针对不同类型的重大网络攻击制定相应的隔离策略；还应建立高效的清除计划流程；制定共享有关网络事件的威胁情报和最佳实践信息。 高：除上述控制外，认可机构应确保负责事件管理职能的人员在事件发生期间与负责网络威胁情报职能的人员能够进行有效协作。在适用的情况下，部署自动化机制以支持事件管理、遏制、清除和恢复流程。	
5.2.3	恢复与质量保证测试	基线：认可机构应建立并验证在及时、安全和弹性地恢复受影响的功能、服务和数据方面的流程有效性。验证系统在恢复后的正常运行状态，修复安全漏洞。开展年度业务连续性和数据恢复测试，验证系统和数据的完整性和可用性。 中：除上述控制外，认可机构应建立流程，确保恢复后的 IT 资产经过重新配置与全面测试；持续跟踪网络事件进展并向管理层定期汇报；对关键在线系统进行压力测试，验证高负载下的稳定性；在弹性测试中纳入现实且可能发生的新兴网络威	**在基础设施的恢复能力方面**，腾讯云数据中心遍布全球多个区域，其中三个数据中心部署在香港境内，供客户选择和部署。每个可用区的网络出口对接多个运营商，构建腾讯云网络跨地域的灾备能力，有效降低运营商公网故障带来的持续性影响。腾讯云各数据中心的电力系统和空调系统均采用高稳定性全冗余系统，以避免单点故障影响数据中心的电力和供冷持续性。腾讯云基础网络和计算节点均采用冗余建设方式，确保网络服务和客户业务的有效性，不会因单点故障而中断。

编号	控制域	控制要求总结	腾讯云的应答
		胁场景。 高：除上述控制外，认可机构应每年至少开展一次覆盖所有关键业务职能的网络事件响应与恢复演练；在恢复站点运行关键业务足够时间，验证其实际支撑能力；建立流程，彻底解决测试中发现的根本问题；使用可能造成重大损失的网络事件场景进行压力测试；测试不同处理中心或系统之间的切换能力，确保业务连续性。	**为协助客户进行恢复测试和演练**，腾讯云提供了**云顾问（TSA）**服务。该服务是多个ITOM 领域垂直应用的云上治理平台，依托腾讯云海量运维专家经验，通过风险巡检、故障演练等多重治理优化云基础设施。TSA 能够提供 IaaS 到 PaaS 各类故障注入场景，以及多个行业的演练经验模板，覆盖跨可用区容灾等多个典型应用场景，帮助客户根据自身业务需求，快速高效复用成熟解决方案，提高系统的可用性。客户还可选用**云压测（PTS）**服务，通过模拟海量用户的真实业务场景，全方位验证系统可用性和稳定性。PTS 可提供百万并发多地域流量发起能力，以及流量录制、场景编排、流量定制、高级脚本定制等功能，可快速根据业务模型定义压测场景，真实还原应用大规模业务访问场景，帮助客户提前识别应用性能问题。 腾讯云内部亦会每年进行业务连续性相关的培训和演练。演练时以业务连续性计划为基础制定演练方案，基于测试目标及范围进行演练风险评估，并制定相应的保障措施，避免因演练对服务造成负面影响。腾讯云定期通过模拟真实的经典容灾场景进行灾难恢复演练，包括攻防对抗和大规模故障等，全面检查系统的容灾能力、响应速度和恢复能力，确保在突发状况发生时，业务可以迅速恢复正常。

5.5.3 网络取证

编号	控制域	控制要求总结	腾讯云的应答
5.3.1	证据收集流程	基线：认可机构应建立详细的证据收集流程和制定正式的、成文的程序，以确保事件相关证据的正确收集与保存 中：除上述控制外，认可机构应确保	**为协助客户进行事件相关证据的收集、汇总和分析**，腾讯云提供了**日志服务（CLS）**。作为一站式日志服务平台，CLS 提供了从日志采集、日志存储到日志检索分析、实时消费、

编号	控制域	控制要求总结	腾讯云的应答
		信息系统使用内部系统时钟为审计记录生成时间戳，时间戳具有足够的细粒度（如精确到毫秒），满足内部使用和外部用途（如监管审查、法律诉讼等）的需求。 高：N/A。	日志投递等多项服务，协助客户解决业务运营、安全监控、日志审计、日志分析等问题。CLS 采用高可用的分布式架构设计，对日志数据进行了多冗余备份存储，防止单节点服务宕机数据不可用，实现服务的高可用性， 为日志数据提供稳定可靠的服务保障。**云安全中心（CSC）**亦支持采集云安全产品告警 数据、云资产配置变更数据、云上用户操作行为数据及部分云产品日志数据等各类云上安全相关数据，并提供统一检索调查平台，帮助客户实现全面的云上日志审计与检 索调查。此外，**Elasticsearch Service (ES)** 服务，将云服务器、容器等其他云产品实时日志，或业务的存量及增量业务数据，汇聚传输到腾讯云 ES 集群，进行数据的分布式存储、查询分析。 **针对网络日志的收集与留存**，**云防火墙（CFW）**支持全流量的网络日志分析，最高 可留存 6 个月。并支持高级威胁溯源分析，可分析域名的注册、解析、备案及历史解析信息。 **针对操作日志的收集与留存**，客户可采用**操作审计 (CloudAudit)**对腾讯云账号活动进 行监管、合规性检查、操作审核和风险审核。CloudAudit 支持在线查看 90 天以内的腾讯云控制台和云 API 操作记录，包括访问密钥、区域、错误码、事件 ID、事件名称、事件源、事件时间、请求 ID、源 IP 地址、
5.3.2	需收集的证据类型	基线：认可机构应建立证据收集流程，确保收集的数字和取证证据来源能够为事后的安全事件调查和分析提供有效支撑。 中：除上述控制外，认可机构需要确保所收集的数字和取证证据范围全面且符合当前的业务需求和风险状况。定期对所收集的数字和取证证据范围、证据保存期间进行审查。 高：除上述控制外，认可机构应基于风险评估方法，对数字和取证证据范围进行审查与更新。在信息系统发生重大变更或出现新的网络威胁与漏洞时，应立即触发对数字和取证证据范围的审查与更新。	
5.3.3	调查和分析证据的过程	基线：认可机构应安排具备资质的内部人员或第三方机构执行证据的安全调查、取证分析和修复工作。 中：除上述控制外，认可机构安排的专家应能够结合业务影响分析，清晰阐述网络事件对业务造成的大致影响的相关情况。 高：除上述控制外，认可机构应建立安全调查与取证分析流程，并基于风险评估方法来判断应采取实时响应还是 离线介质分析。	

编号	控制域	控制要求总结	腾讯云的应答
5.3.4	保护证据	基线：认可机构应建立控制措施，限制对证据未经授权的访问权限。 中：除上述控制外，认可机构应明确限定可访问证据的用户名单，并对其实施受限访问。 高：除上述控制外，认可机构应实施监控机制，以检测对证据的未经授权访问行为。	用户名。 **为配合客户遵从监管要求，在事件管理与证据收集方面**，腾讯云内部明确了安全事件证据收集的相关标准。在信息安全事件受理、调查评估、处理、跟踪的过程中，相关责任部门会维护所受理的信息安全事件的相关记录，并确保记录的完整性和保密性。腾讯云会根据客户的需求，在评估合理性和可行性的基础上，为客户的数字取证和事后安全事件调查和分析提供有效支持。 **在日志管理方面**，腾讯云建立了日志收集与管理规范及机制，对登录日志、操作日志、系统常规日志、系统安全事件日志等日志的记录、提取、存储、防护、分析、审计等进行管控，以检测和防范系统活动异常和风险。日志统一归集至腾讯云日志管理平台进行管理，并对相关日志信息采取备份和严格的保护措施，防止受到未经授权的修改和删除，备份日志保存时间超过一年。腾讯云通过运维安全自动化审计工具和内部审计团队对日志进行审计，检测系统或操作异常，以防范操作风险。 **针对时间戳**，由于时间戳的准确性和一致性关系到日志信息的有效性，腾讯云定期检查 NTP 服务器的时间同步情况，确保全网时间统一、准确、可靠。
5.3.5	证据的保留和存储	基线：认可机构应明确定义证据的保留期限。 中：除上述控制外，认可机构应建立适当的流程，确保证据根据需要存储或归档证据。 高：N/A	

5.5.4 沟通与改进

编号	控制域	控制要求总结	腾讯云的应答
5.4.1	事件升级机制	基线：认可机构应建立流程，用于向相关利益相关方（如管理层、IT 团队、法务部门等）通报潜在网络安全事件。 中：除上述控制外，认可机构应建立的沟通计划，其中包含在发生可能	**为配合客户有效履行沟通与告知义务**，腾讯云制定了信息安全事件管理规范，建立了信息安全事件响应、事件升级、事件通知等相关程序，以及时向可能或已经受到事故影响的公司内部人员、客户等相关方进行预警或

编号	控制域	控制要求总结	腾讯云的应答
		影响其他组织或其客户的安全事件，也包括向媒体通报事件的程序。 高：N/A。	通知，确保各方能够有序、及时、高效地进行沟通协调。 对于可能影响到客户的安全事件，腾讯云会根据信息安全事件的影响范围和程度，在经过内部评审后，将信息安全事件的处理和分析结果通过合适的方式通知客户，并提供相应的技术支持，以协助客户采取补救措施以将损失降到最低。
5.4.2	事件报告	基线：认可机构应建立正式的流程，定期向必要利益相关方提交安全事件报告。 中：除上述控制外，认可机构制定网络安全事件的报告其中一部分应包含详细指标、仪表盘。 高：认可机构应引入自动化机制辅助安全事件的报告工作，用于提升事件加快上报、报告和响应速度和效率。	**在客户向腾讯云报告问题或主动联络方面**， 腾讯云通过腾讯云官网控制台提供工单服务，支持客户报告与安全、可用性和保密相关的故障、事件、问题和投诉。腾讯云工单系统会通过分级响应机制对客户工单分配优先级，当一线技术团队无法有效解决时，系统将自动触发服务升级流程，由产品或技术团队介入协同处理，确保客户的需求或反馈获得及时响应与处理。 腾讯云在官方网站上提供了在线及电话通道，支持客户反馈使用腾讯云服务时遇到的问题。腾讯云拥有多地域互备的客户服务中心，能够 7*24 不间断地处理来自客户的咨询或需求，**提供高质量、全天候的技术支持。**此外，客户还可以选择适用的服务计划，获取专属支持群、专属技术服务经理、增值服务等组成的专属支持。
5.4.3	持续改进	基线：认可机构应建立正式且持续的改进流程，用于识别从过去的网络事件处理活动中总结出的经验教训。 中：除上述控制外，认可机构应定期开展模拟测试与演练，以评估事件响应和恢复能力，在应对常见报道事件及不同场景下的准备情况。 高：除上述控制外，认可机构应定期参考所有安全事件，执行趋势分析，这有助于改进网络安全措施和政策。	**在事件总结与持续改进方面**，腾讯云建立了 周期性的事件分析机制，会定期对事件进行多维分析（事件类型、发生频次、影响范围及严重程度），并基于事件复盘与根因分析采取预防措施，防止类似事件再次发生。针对重大安全事件，腾讯云会成立专责小组形成专项分析报告向管理层进行汇报。

5.6 领域六：态势感知

5.6.1 威胁情报

编号	控制域	控制要求总结	腾讯云的应答
6.1.1	威胁情报	基线：认可机构应订阅威胁情报共享来源，并用威胁情报来监控相关的网络威胁，以此增强其网络安全风险管理和控制能力。 中：除上述控制外，认可机构应实施正式的网络威胁情报计划，定期评估现有外部网络情报监测服务，制定信息收集协议，用于收集同行业和政府机构的信息，维护集中式的网络只读威胁情报库。 高：除上述控制外，认可机构应建立网络情报框架，实施正式的威胁情报计划，能够实时从多个来源自动获取威胁情报，同时实施威胁分析系统，对各类威胁数据进行关联分析，向管理层发出告警。	为支持客户进行威胁检测与分析，腾讯向客户提供了**威胁情报中心（TIX）**。作为一站式情报服务平台，威胁情报中心可提供基础情报、攻击面情报、业务情报三大情报能力，支持情报查询、IOC 研判分析、攻击面管理等功能，能够协助客户更高效地对安全事件进行分析研判，和更全面地评估企业资产暴露面的风险情况，助力企业构建高效的立体化安全防御体系。威胁情报中心构建了完整的情报触点网，从漏洞社区、安全机构、安全工具厂商、社交媒体、安全博客等多种来源收集和分析威胁情报，并联动云端算法算力去除误报，保障了情报的准确性。 此外，威胁情报中心以 SaaS 化为核心，支持 Web 端 API、SDK、TIP、小程序等多种交付方式，满足不同客户需求。威胁情报中心还可以通过被集成方式，将云端情报数据与客户现有的安全防护产品进行联动，以提高整体安全运营和威胁响应效率。 基于威胁情报中心的赋能与支持，腾讯云致力于构建“情报-攻防-管理-规划”的主动防御安全能力体系，通过整合威胁情报、人工智能、大数据等技术，提升安全事件的响应能力和效率，并设立了 7×24 小时安全运营中心，聚焦威胁检测、调查和响应，实现安全态势的可知、可见、可控。

5.7 领域七：第三方风险管理

5.7.1 外部连接

编号	控制域	控制要求总结	腾讯云的应答
7.1.1	识别	基线：认可机构应识别所有依赖于外部连接或网络连接第三方及其关键业务流程，应绘制网络与系统数据流向图，并进行定期审查和更新。 中：除上述控制外，认可机构应识别和评估外部连接及网络连接的第三方的相关风险。 高：除上述控制外，认可机构应对识别到的潜在风险实施安全性影响评估并形成书面记录，确保不会引入新的风险。	**为支持客户的网络通信安全**，腾讯云部署了成熟的网络安全架构，通过防火墙、入侵检测/防御系统（IDS/IPS）、DDoS 防护、网络逻辑隔离、Web 应用安全等多重防护机制，及时检测、过滤并阻止恶意网络流量，保护腾讯云的网络安全。客户在腾讯云控制台上的通信均受到 HTTPS 安全协议的加密保护，腾讯云的云产品所提供的云 API 接口具有 HTTPS 加密、签名校验、状态监测等安全能力，能为客户的业务提供端口级别的通信安全保障。腾讯云还为客户提供**私有网络（VPC）**，能够基于隧道技术，在物理网络上构造虚拟网络，并使用虚拟化技术，实现不同私有网络间完全逻辑隔离。作为隔离的网络环境，私有网络支持客户通过设置安全组和网格 ACL 实现访问流量控制，并支持通过访问管理（CAM）实现最小授权。 此外，客户还可选用腾讯云提供的其他服务以进一步强化网络边界防护和确保数据传输的安全性，包括**专线接入（DC）**、**VPN 连接 (VPN Connection)**、**云防火墙 (CFW)**、**Web 应用防火墙（WAF）**等。有关网络边界防护的更多信息请参考本指南**第 5.3.2 章节“基础设施保护控制”。** **针对云租户的访问隔离**，腾讯云通过多层次的技术隔离手段，如虚拟化控制层资源访问控制策略、云平台内部私有网络间隔离策略、Web 控制台权限分配与身份验证、接口会话 ID 与访问密钥等安全机制，确保客户数据互不可见，从技术上保证租户不能访问、获取或篡改其他租户的数据。
7.1.2	保护	基线：认可机构应建立并维护统一、全面的安全边界防护框架，所有对外连接必须通过配置了边界设备的受控接口。 中：除上述控制外，认可机构应限制非必要的外部网络连接，系统访问仅在业务需要的基础上授予，并遵循“最小权限原则”。 高：除上述控制外，认可机构的出站流量通过预定义的网络控制点（例如 Web 代理）进行路由，由网络安全部署对入站流量进行保护；建立集中管理的控制台或界面来监控和管理代理服务器；并且采用边界防护机制。	

5.7.2 第三方管理&第三方风险的持续监测

编号	控制域	控制要求总结	腾讯云的应答
7.2.1	合同管理	基线：认可机构应与处理、存储或传输其敏感或关键数据的第三方签订合同，合同中明确对第三方的安全性和隐私性承担责任；在合同终止后，对认可机构的敏感或关键数据进行归还或销毁所需遵循的安全要求。 中：除上述控制外，认可机构应在与第三方的合同或服务级别协议（SLA）中约定网络安全事件和漏洞通知的义务。 高：除上述控制外，认可机构应与第三方建立终止合作/退出策略，退出策略需要定期进行测试，将中等风险和高风险事项及其对应的处理方法提交管理层审批确认。	腾讯云作为云服务提供商，提供了线上的《服务条款》、《服务等级协议》、《数据处理和安全协议》等法律文档，对腾讯云所提供服务的内容和服务水平、用户数据和知识产权的保护、客户与腾讯云双方的安全责任与义务、事件和变更的通知、保密责任以及信息披露事宜等进行了明确。客户还可以协商将额外的要求写入单独的合同中。 若客户因业务变更或未来 IT 规划需要终止合同协议，可以选择在任何时间对云端数据和生产环境进行备份和迁移。腾讯云支持客户采用通用的标准格式来备份或迁移数据，故客户能够采用与上云阶段相同的传输方式和传输协议，或使用**专线接入 (DC)**、**VPN 连接 (VPN Connection)** 等网络服务产品，确保数据在下云阶段时安全可靠。当客户的云服务终止后，腾讯云遵循严格的数据擦除方式，在保留期限届满后彻底删除包括副本和备份在内的客户数据，删除后的数据无法复原。
7.2.2	尽职调查	基线：认可机构应对合作意向的第三方开展网络安全控制的尽职调查。 中：除上述控制外，认可机构应定期对第三方服务提供商进行安全评估或审计。 高：除上述控制外，认可机构应建立定期评估分包商网络安全状况的程序。	为配合客户的尽职调查及外包监察要求，腾讯云将依据实际情况及与客户的协议和约定，配合客户的第三方安全审计和监督，并提供专人协助，积极响应及配合客户发起的审计活动。同时，腾讯云安全团队每年至少进行一次内部安全审计，并持续监控云平台和内部系统的情况，确保其保持良好的安全态势，符合相关法律法规及安全管理标准的规定和要求。腾讯云也每年接受独立第三方的专业审计，并通过提供具有鉴证性质的系统与组织控制报告，向云用户机构、独立审计师、监管机构、公司股东及其他相关利益方公开腾讯云最新的服务组织内部控制情况。 腾讯云已为国际众多企业和政府机构提供了可靠的云计算服务，受到全球不同行业客户的认可，并获得了多项国内外行业机构的专业认证。腾讯云承诺其服务符合行业标准和法律法规要求。基于相关的国际标准，腾
7.3.1	第三方风险的持续监测	基线：认可机构建立针对网络连接且处理、存储或传输敏感或关键数据的第三方定期监测程序。 中：除上述控制外，认可机构监测的深度和频率应根据第三方的风险等级进行相应调整。 高：除上述控制外，认可机构应定期对第三方开展现场评估或审查审计	

编号	控制域	控制要求总结	腾讯云的应答
		报告，且依据“最小权限原则”主动对第三方员工在认可机构自建系统及第三方托管系统中访问认可机构的敏感或关键数据的行为进行追踪与管理。	讯云建立了信息安全管理体系、隐私保护管理体系、业务连续性管理体系等，并在内部定期开展审查和风险评估，确保体系要求落地。 若腾讯云涉及到将相关业务进行分包，腾讯云会及时通知客户，并根据实际情况与客户在协议中约定分包相关的条款，对分包进行管理。同时，腾讯云会积极配合客户的外包管理要求，积极响应及配合客户方发起的审计或评估活动等。在分包商管理方面，腾讯云建立了完善的供应链安全管理体系，通过严格的供应商安全评估和准入、定期监察与评估，以及明确的外包服务协议等措施，确保对供应商的有效管控。

06 结语

腾讯云是腾讯集团倾力打造的云计算品牌，承接腾讯多年的技术积累与安全实践能力。腾讯云致力于为客户持续提供安全、可信、智慧的云，助力更多企业高效迎接数字化浪潮，推进企业安全发展。

本指南基于香港金管局《C-RAF 2.0》中网络安全成熟度评估的控制目标及原则，向客户全面、透明地展示腾讯云如何协助客户实现云上系统和数据的合规，助力企业客户放心、安心地将系统和数据托管上云。腾讯云希望能通过本指南，支持企业客户有效满足金管局《C-RAF 2.0》网络安全成熟度标准，同时高效实现数字化升级和业务的创新发展。

本指南仅供参考。对于本指南中的信息，客户可结合自身实际情况酌情使用，以确保在使用腾讯云云服务过程中的监管合规性。

07 版本历史

日期	版本	详情
2026 年 4 月	V1.0	首次发布