CSA cloud security alliance®

CSA GCR GREATER CHINA REGION cloud security alliance®

CCM™ 云控制矩阵4.0（中英版）

Cloud Controls Matrix v4

中文翻译版说明

本文由云安全联盟大中华区（CSA GCR）CCM4.0翻译专家组对《Cloud Controls Matrix v4》进行翻译审校。

翻译审校工作专家（以下排名按字母先后排序）

陈皓 顾伟 高铁峰 胡友杰 苏泰泉 沈勇 王永霞 于新元 赵锐

Control Title 控制措施	Control ID 控制编号	Updated Control Specification 更新的控制措施规范
Audit & Assurance - A&A 审计&保障		
Audit and Assurance Policy and Procedures 审计与保障的策略及规程	**A&A-01**	Establish, document, approve, communicate, apply, evaluate and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护审计和保障策略、规程和标准。至少每年一次审查和更新公司的策略和规程。
Independent Assessments 独立评估	**A&A-02**	Conduct independent audit and assurance assessments according to relevant standards at least annually. 每年至少一次，根据相关标准进行独立审计和保障评估
Risk Based Planning Assessment 基于风险规划评估	**A&A-03**	Perform independent audit and assurance assessments according to risk-based plans and policies. 根据基于风险的计划和策略执行独立的审计和保证评估
Requirements Compliance 符合性需求	**A&A-04**	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit. 验证符合所有适用于审计的相关标准、法规、法律/合同和法定要求
Audit Management Process 审计管理过程	**A&A-05**	Define and implement an Audit Management process to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence. 定义和实施审计管理过程，以支持审计计划、风险分析、安全控制评估、结论、补救计划、报告生成，以及对过去报告和相关证据的审查。
Remediation 补救	**A&A-06**	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders. 建立、记录、批准、沟通、应用、评估和维护基于风险的纠正行动计划，以修正审计发现，审查并向相关利益相关者报告修正状况。
Application & Interface Security - AIS 应用程序和接口安全		
Application and Interface Security Policy and Procedures 应用和接口安全策略和规程	**AIS-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、申请、评估和维护应用程序安全策略和规程，为组织的应用程序安全能力的适当规划、交付和支持提供指导。每年至少一次审查和更新公司的策略和规程。
Application Security Baseline Requirements 应用程序安全基线需求	**AIS-02**	Establish, document and maintain baseline requirements for securing different applications. 建立、记录和维护保护不同应用程序的基线要求。
Application Security Metrics 应用程序安全指标	**AIS-03**	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations. 根据业务目标、安全需求和合规义务， 定义和实施技术和运行的指标。
Secure Application Design and Development 应用程序安全设计和开发	**AIS-04**	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization. 根据组织定义的安全需求，定义并实现应用程序设计、开发、部署和运行的SDLC过程
Automated Application Security Testing 自动应用程序安全测试	**AIS-05**	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible. 实现一个测试战略，包括新的信息系统、升级和新版本的接受准则，这提供了应用程序的安全保障，并在实现组织交付速度目标的同时保持遵从性。在适用和可能的情况下，自动化。
Automated Secure Application Deployment 自动应用程序安全部署	**AIS-06**	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible. 为安全、标准化和兼容的应用程序部署建立和实施战略和能力。尽可能自动化。

Application Vulnerability Remediation 应用程序漏洞修复	**AIS-07**	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible. 定义并实施修复应用程序安全脆弱性的过程，并在可能时自动修复。
Business Continuity Management and Operational Resilience - BCR 业务连续性管理和运营弹性		
Business Continuity Management Policy and Procedures 业务连续性管理策略和规程	**BCR-01**	Establish, document, approve, communicate, apply, evaluate and maintain business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually. 建立、归档、批准、沟通、应用、评估和维护业务连续性管理和运营弹性策略和规程。每年至少审查和更新公司的策略和规程。
Risk Assessment and Impact Analysis 风险评估和影响分析	**BCR-02**	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities. 确定业务中断的风险和影响，为开发业务连续性和运营弹性策略和能力建立标准。
Business Continuity Strategy 业务连续性策略	**BCR-03**	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite. 在风险偏好范围内建立战略，以减少、抵御和恢复业务中断的影响。
Business Continuity Planning 业务连续性计划	**BCR-04**	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities. 建立、记录、批准、沟通、应用、评估和维护基于运营弹性策略和能力结果的业务连续性计划。
Documentation 文档记录	**BCR-05**	Develop, identify, and acquire documentation that is relevant to support the business continuity and operational resilience programs. Make the documentation available to authorized stakeholders and review periodically. 开发、识别和获取与支持业务连续性和运营弹性计划相关的文件。将文件提供给授权的利益相关者，并定期审查。
Business Continuity Exercises 业务连续性的演习	**BCR-06**	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes. 至少每年或在重大变更时， 对业务连续性和运营弹性计划进行测试和演习。
Communication 沟通	**BCR-07**	Establish communication with stakeholders and participants in the course of business continuity and resilience procedures. 在业务连续性和韧性规程的过程中与利益相关者和参与者建立沟通。
Backup 备份	**BCR-08**	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency. 定期备份存储在云中的数据。确保备份的机密性、完整性和可用性；并为了韧性，验证从备份恢复的数据。
Disaster Response Plan 灾难响应计划	**BCR-09**	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes. 建立、记录、批准、沟通、应用、评估和维护灾难响应计划，以从自然和人为灾害中恢复。至少每年更新一次计划，或在重大变更时更新。
Response Plan Exercise 响应计划演习	**BCR-10**	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities. 每年或发生重大变化时演练灾难响应计划，如果可能，联合当地应急官方机构
Equipment Redundancy 设备冗余	**BCR-11**	Supplement business-critical equipment with redundant equipment independently located at a reasonable minimum distance in accordance with applicable industry standards. 根据适用的行业标准，用独立设置的、合理的最小距离的冗余设备补充关键业务设备。
Change Control and Configuration Management - CCC 变更控制和配置管理		
Change Management Policy and Procedures 变更管理策略和规程	**CCC-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护用于变更管理的策略和规程，为管理申请变更对组织的相关风险，包括应用程序、系统、基础设施、配置等，无论资产是在内部管理还是在外部管理 （即外包）。 至少每年审查和更新公司的策略和规程。
Quality Testing 质量测试	**CCC-02**	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards. 遵循已制定的质量变更控制、批准和测试过程，以及已建立的基线、测试和发布标准。

Change Management Technology 变更管理技术	**CCC-03**	Manage the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration, etc., regardless of whether the assets are managed internally or externally (i.e., outsourced). 通过变更管理技术来管理组织资产变更相关的风险，包括应用程序、系统、基础架构、配置等，无论资产是内部管理的还是外部管理的（即外包）。
Unauthorized Change Protection 未经授权的变更保护	**CCC-04**	Restrict the unauthorized addition, removal, update, and management of organization assets. 实施变更管理技术，限制未经授权添加、删除、更新和管理组织资产。
Change Agreements 变更协议	**CCC-05**	Include provisions limiting changes directly impacting CSCs owned environments/tenants to explicitly authorized requests within service level agreements between CSPs and CSCs. 对于直接影响客户环境或租户环境的变更，在云服务提供商（CSP）和客户（CSC）间的服务水平协议中，要包含限制条款，以明确授权请求。
Change Management Baseline 变更管理基线	**CCC-06**	Establish change management baselines for all relevant authorized changes on organization assets. 对于所有组织资产的变更授权建立变更管理基线。
Detection of Baseline Deviation 基线偏差检测	**CCC-07**	Implement detection measures with proactive notification in case of changes deviating from the established baseline. 实施基线偏离检测，在在发生偏离既定基线的变化时主动告警。
Exception Management 例外管理	**CCC-08**	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process. Align the procedure with the requirements of GRC-04: Policy Exception Process. 在变更和配置过程中实施一个例外管理规程（包括紧急情况）。 该规程与“GRC-04：策略例外过程”的要求一致。
Change Restoration 变更恢复	**CCC-09**	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns. 定义并实施过程，在变更出现错误或安全问题时主动回退，并将系统/服务恢复到上一个已知的良好状态。
Cryptography, Encryption & Key Management 密码学、加密与密钥管理		
Encryption and Key Management Policy and Procedures 密码学、加密与密钥管理的策略及规程	**CEK-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Cryptography, Encryption and Key Management. Review and update the policies and procedures at least annually. 制定、记录、批准、交流、应用、评估和维护密码学、加密与密钥管理的策略及规程。至少每年审查和更新策略及规程。
CEK Roles and Responsibilities 密码学、加密与密钥管理的作用及责任	**CEK-02**	Define and implement cryptographic, encryption and key management roles and responsibilities. 定义并实施密码学、加密与密钥管理的角色及责任。
Data Encryption 数据加密	**CEK-03**	Provide cryptographic protection to data at-rest and in-transit, using cryptographic libraries certified to approved standards. 使用经过标准认证的密码（算法）库，为静态和传输中的数据提供密码保护。
Encryption Algorithm 加密算法	**CEK-04**	Use encryption algorithms that are appropriate for data protection, considering the classification of data, associated risks, and usability of the encryption technology. 考虑数据分级、相关风险和加密技术的可用性，使用适合数据保护的加密算法。
Encryption Change Management 加密变更管理	**CEK-05**	Establish a standard change management procedure, to accommodate changes from internal and external sources, for review, approval, implementation and communication of cryptographic, encryption and key management technology changes. 建立标准的变更管理规程，以适应来自内部和外部的变更，用于审查、批准、执行和通报密码学、加密与密钥管理技术的变更。
Encryption Change Cost Benefit Analysis 加密变更成本效益分析	**CEK-06**	Manage and adopt changes to cryptography-, encryption-, and key management-related systems (including policies and procedures) that fully account for downstream effects of proposed changes, including residual risk, cost, and benefits analysis. 管理和采用对密码学、加密与密钥管理相关系统（包括策略及规程）的变更，以充分考虑拟议变更的下游影响，包括剩余风险、成本和效益分析。

Encryption Risk Management 加密风险管理	**CEK-07**	Establish and maintain an encryption and key management risk program that includes provisions for risk assessment, risk treatment, risk context, monitoring, and feedback. 建立并维护一个加密和密钥管理风险程序，包括风险评估、风险处理、风险关联、监控和反馈的规定。
CSC Key Management Capabiility CSC密钥管理能力	**CEK-08**	CSPs must provide the capability for CSCs to manage their own data encryption keys. 云服务提供商（CSP）必须为客户（CSC）提供管理自己的数据加密密钥的能力。
Encryption and Key Management Audit 加密与密钥管理审计	**CEK-09**	Audit encryption and key management systems, policies, and processes with a frequency that is proportional to the risk exposure of the system with audit occurring preferably continuously but at least annually and after any security event(s). 审计加密和密钥管理系统、策略和规程的频率与系统的风险暴露程度成正比，审计最好是连续进行，但至少每年一次，并在任何安全事态后进行。
Key Generation 密钥生成	**CEK-10**	Generate Cryptographic keys using industry accepted cryptographic libraries specifying the algorithm strength and the random number generator used. 使用行业认可的密码（算法）库生成加密密钥，指定算法强度和使用的随机数生成器。
Key Purpose 密钥用途	**CEK-11**	Manage cryptographic secret and private keys that are provisioned for a unique purpose. 管理为特殊用途而准备的密钥和私钥。
Key Rotation 密钥轮换	**CEK-12**	Rotate cryptographic keys in accordance with the calculated cryptoperiod, which includes provisions for considering the risk of information disclosure and legal and regulatory requirements. 按照计算出的加密周期轮换密钥，其中包括考虑信息披露风险和法律及监管要求的规定。
Key Revocation 密钥废除	**CEK-13**	Define, implement and evaluate processes, procedures and technical measures to revoke and remove cryptographic keys prior to the end of its established cryptoperiod, when a key is compromised, or an entity is no longer part of the organization, which include provisions for legal and regulatory requirements. 定义、执行和评估在既定的加密期结束前、在密钥泄密时或在某一实体不再是组织的一部分时，撤销及删除密钥的过程、规程和技术措施，其中包括法律和监管要求的规定。
Key Destruction 密钥销毁	**CEK-14**	Define, implement and evaluate processes, procedures and technical measures to destroy keys stored outside a secure environment and revoke keys stored in Hardware Security Modules (HSMs) when they are no longer needed, which include provisions for legal and regulatory requirements. 定义、执行和评估销毁储存在安全环境之外的密钥和在不再需要时撤销储存在硬件安全模块中的密钥的过程、规程和技术措施，其中包括法律和监管要求的规定。
Key Activation 密钥激活	**CEK-15**	Define, implement and evaluate processes, procedures and technical measures to create keys in a pre-activated state when they have been generated but not authorized for use, which include provisions for legal and regulatory requirements. 定义、执行和评估在密钥已生成但未被授权使用时，在预激活状态下生成密钥的过程、规程和技术措施，其中包括法律和监管要求的规定。
Key Suspension 密钥停止	**CEK-16**	Define, implement and evaluate processes, procedures and technical measures to monitor, review and approve key transitions from any state to/from suspension, which include provisions for legal and regulatory requirements. 定义、执行和评估监测、审查和批准密钥从任何状态到/从暂停状态的关键过渡的过程、规程和技术措施，其中包括法律和监管要求的规定。
Key Deactivation 密钥注销	**CEK-17**	Define, implement and evaluate processes, procedures and technical measures to deactivate keys at the time of their expiration date, which include provisions for legal and regulatory requirements. 定义、执行和评估在密钥到期时停用密钥的过程、规程和技术措施，其中包括法律和监管要求的规定。
Key Archival 密钥归档	**CEK-18**	Define, implement and evaluate processes, procedures and technical measures to manage archived keys in a secure repository requiring least privilege access, which include provisions for legal and regulatory requirements. 定义、执行和评估管理需要最低权限访问的安全储存库中已归档密钥的过程、规程和技术措施，其中包括法律和监管要求的规定。
Key Compromise 密钥泄密	**CEK-19**	Define, implement and evaluate processes, procedures and technical measures to use compromised keys to encrypt information only in controlled circumstance, and thereafter exclusively for decrypting data and never for encrypting data, which include provisions for legal and regulatory requirements. 定义、执行和评估仅在受控情况下使用泄密密钥对信息进行加密，及此后仅用于对数据进行解密，绝不用于对数据进行加密的过程、规程和技术措施，其中包括法律和监管要求的规定。

Key Recovery 密钥找回	**CEK-20**	Define, implement and evaluate processes, procedures and technical measures to assess the risk to operational continuity versus the risk of the keying material and the information it protects being exposed if control of the keying material is lost, which include provisions for legal and regulatory requirements. 定义、执行和评估在失去对密钥材料的控制时，业务连续性风险与密钥材料及其保护的信息暴露风险的过程、规程和技术措施，其中包括法律和监管要求的规定。
Key Inventory Management 密钥清单管理	**CEK-21**	Define, implement and evaluate processes, procedures and technical measures in order for the key management system to track and report all cryptographic materials and changes in status, which include provisions for legal and regulatory requirements. 定义、执行和评估使密钥管理系统能够跟踪和报告所有密码材料和状态的变化的过程、规程和技术措施，其中包括法律和监管要求的规定。
Datacenter Security - DCS 数据中心安全		
Off-Site Equipment Disposal Policy and Procedures 处置场外设备的策略和规程	**DCS-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises. If the equipment is not physically destroyed a data destruction procedure that renders recovery of information impossible must be applied. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护用于安全处置组织场所以外设备的策略和规程。如果设备未被物理销毁，则必须采用数据销毁规程，使信息无法恢复。 每年至少审查和更新公司的策略和规程。
Off-Site Transfer Authorization Policy and Procedures 场外传输授权策略和规程	**DCS-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the relocation or transfer of hardware, software, or data/information to an offsite or alternate location. The relocation or transfer request requires the written or cryptographically verifiable authorization. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护用于硬件、软件或数据/信息搬迁或传输到场外或备用位置的策略和规程。搬迁或传输到场外之前必须经过书面或可加密验证的授权。 至少每年一次审查和更新公司的策略和规程。
Secure Area Policy and Procedures 安全区策略和规程	**DCS-03**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for maintaining a safe and secure working environment in offices, rooms, and facilities. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护用于办公室、房间和设施内维护安全工作环境的策略和规程。至少每年一次审查和更新公司的策略和规程。
Secure Media Transportation Policy and Procedures 安全的媒介传输策略和规程	**DCS-04**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the secure transportation of physical media. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护用于安全传输物理媒介的策略和规程。 至少每年一次审查和更新公司的策略和规程。
Assets Classification 资产分级	**DCS-05**	Classify and document the physical, and logical assets (e.g., applications) based on the organizational business risk. 根据组织业务风险对物理和逻辑资产（例如应用程序）进行分级和记录。
Assets Cataloguing and Tracking 资产分类与跟踪	**DCS-06**	Catalogue and track all relevant physical and logical assets located at all of the CSP's sites within a secured system. 记录并跟踪每一个安全系统中所有位于云服务提供商站点的所有物理和逻辑资产。
Controlled Access Points 受控接入点	**DCS-07**	Implement physical security perimeters to safeguard personnel, data, and information systems. Establish physical security perimeters between the administrative and business areas and the data storage and processing facilities areas. 实施物理安全边界以保护人员、数据和信息系统。 在管理区域和业务区域以及数据存储区域和数据处理区域之间建立物理安全边界。
Equipment Identification 设备标识	**DCS-08**	Use equipment identification as a method for connection authentication. 使用设备标识作为连接身份鉴别的方法。
Secure Area Authorization 安全区域授权	**DCS-09**	Allow only authorized personnel access to secure areas, with all ingress and egress points restricted, documented, and monitored by physical access control mechanisms. Retain access control records on a periodic basis as deemed appropriate by the organization. 只允许授权人员访问安全区域，通过物理访问控制机制限制、记录和监视所有入口和出口。按组织要求保留访问控制记录。
Surveillance System 监视系统	**DCS-10**	Implement, maintain, and operate datacenter surveillance systems at the external perimeter and at all the ingress and egress points to detect unauthorized ingress and egress attempts. 在外部边界以及所有入口和出口点实施、维护和运行数据中心监视系统，以检测未经授权的出入尝试。

Unauthorized Access Response Training 未授权访问响应培训	**DCS-11**	Train datacenter personnel to respond to unauthorized ingress or egress attempts. 培训数据中心的人员响应未授权的出入尝试。
Cabling Security 布线安全	**DCS-12**	Define, implement and evaluate processes, procedures and technical measures that ensure a risk-based protection of power and telecommunication cables from a threat of interception, interference or damage at all facilities, offices and rooms. 定义、实施、评估过程、规程和技术措施，以确保所有设施、办公室、房间的电力和电信电缆有基于风险的保护，不会受到拦截、干扰或损坏的威胁。
Environmental Systems 环境系统	**DCS-13**	Implement and maintain data center environmental control systems that monitor, maintain and test for continual effectiveness the temperature and humidity conditions within accepted industry standards. 实施和维护数据中心环境控制系统，以监控、维护和测试温度和湿度控制的是否符合业界标准以及控制的持续有效性。
Secure Utilities 安全的公用事业	**DCS-14**	Secure, monitor, maintain, and test utilities services for continual effectiveness at planned intervals. 定期监控、维护和测试公用事业（设施）的安全，确保其能够提供持续的服务。
Equipment Location 设备位置	**DCS-15**	Keep business-critical equipment away from locations subject to high probability for environmental risk events. 使关键业务设备远离极易发生环境风险事态的位置。
Data Security and Privacy Lifecycle Management - DSP 数据安全和隐私生命周期管理		
Security and Privacy Policy and Procedures 安全、隐私策略和程序	**DSP-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually. 根据所有适用的法律法规、标准和风险等级，建立、记录、批准、沟通、应用、评估和维护在数据的整个生命周期中对数据进行分级、保护和处理的策略和规程。至少每年审查和更新策略和规程。
Secure Disposal 安全处置	**DSP-02**	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means. 应用业界公认的方法来安全处置存储介质中的数据，使数据无法通过任何取证手段恢复。
Data Inventory 数据清单	**DSP-03**	Create and maintain a data inventory, at least for any sensitive data and personal data. 创建和维护一个至少针对任何敏感数据和个人数据的数据清单。
Data Classification 数据分级	**DSP-04**	Classify data according to its type and sensitivity level. 根据数据类型和敏感程度对数据进行分级。
Data Flow Documentation 数据流文档	**DSP-05**	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change. 创建数据流文档，以确定在何处处理、存储或传输哪些数据。在规定的时间间隔，至少每年，以及在任何变更之后，审查数据流文档。
Data Ownership and Stewardship 数据所有权和管理权	**DSP-06**	Document ownership and stewardship of all relevant documented personal and sensitive data. Perform review at least annually. 记录所有相关记录的个人和敏感数据的所有权和管理权。至少每年进行一次审查。
Data Protection by Design and Default 设计和默认数据保护	**DSP-07**	Develop systems, products, and business practices based upon a principle of security by design and industry best practices. 根据设计安全原则和行业最佳实践，开发系统、产品和业务实践。
Data Privacy by Design and Default 设计和默认数据隐私	**DSP-08**	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations. 根据设计隐私原则和行业最佳实践，开发系统、产品和业务实践。根据所有适用的法律法规，确保系统的隐私设置默认配置。
Data Protection Impact Assessment 数据保护影响评估	**DSP-09**	Conduct a Data Protection Impact Assessment (DPIA) to evaluate the origin, nature, particularity and severity of the risks upon the processing of personal data, according to any applicable laws, regulations and industry best practices. 根据任何适用的法律、法规和行业最佳实践执行数据保护影响评估（DPIA）来评估处理个人数据时风险的来源、性质、特殊性和严重性。
Sensitive Data Transfer 敏感数据传输	**DSP-10**	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations. 定义、实施和评估过程、规程和技术措施，以确保个人或敏感数据在传输中不受未授权访问并且仅在相关法律法规允许的范围内被处理。

Personal Data Access, Reversal, Rectification and Deletion 个人数据访问，撤销，纠正和删除	**DSP-11**	Define and implement, processes, procedures and technical measures to enable data subjects to request access to, modification, or deletion of their personal data, according to any applicable laws and regulations. 根据任何适用的法律法规，定义和实施过程、规程和技术措施，以使数据主体能够请求访问、修改或删除其个人数据。
Limitation of Purpose in Personal Data Processing 个人数据处理中的目的限制	**DSP-12**	Define, implement and evaluate processes, procedures and technical measures to ensure that personal data is processed according to any applicable laws and regulations and for the purposes declared to the data subject. 定义、实施和评估过程、规程和技术措施，以确保个人数据的处理符合任何适用的法律法规和向数据主体声明的目的。
Personal Data Sub-processing 个人数据子处理	**DSP-13**	Define, implement and evaluate processes, procedures and technical measures for the transfer and sub-processing of personal data within the service supply chain, according to any applicable laws and regulations. 根据任何适用的法律法规，定义、实施和评估服务供应链内个人数据传输和子处理的过程、规程和技术措施。
Disclosure of Data Sub-processors 披露数据子处理者	**DSP-14**	Define, implement and evaluate processes, procedures and technical measures to disclose the details of any personal or sensitive data access by sub-processors to the data owner prior to initiation of that processing. 定义、实施和评估过程、规程和技术措施，在数据开始处理之前，向数据所有者披露子处理者访问任何个人或敏感数据的详细信息。
Limitation of Production Data Use 生产数据使用限制	**DSP-15**	Obtain authorization from data owners, and manage associated risk before replicating or using production data in non-production environments. 在非生产环境中复制或使用生产数据之前，请获得数据所有者的授权，并管理相关风险。
Data Retention and Deletion 数据保留和删除	**DSP-16**	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations. 数据保留、归档和删除按照业务要求和适用的法律法规进行管理。
Sensitive Data Protection 敏感数据保护	**DSP-17**	Define and implement, processes, procedures and technical measures to protect sensitive data throughout it's lifecycle. 定义和实施过程、规程和技术措施，以在敏感数据的整个生命周期中保护敏感数据。
Disclosure Notification 披露通知	**DSP-18**	The CSP must have in place, and describe to CSCs the procedure to manage and respond to requests for disclosure of Personal Data by Law Enforcement Authorities according to applicable laws and regulations. The CSP must give special attention to the notification procedure to interested CSCs, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation. 云服务提供商必须制定并向云服务客户说明管理和响应执法机构根据适用法律法规披露个人数据请求的规程。云服务提供商必须特别注意向感兴趣的云服务客户发出通知的规程，除非另有禁止，例如刑法禁止为执法调查保密。
Data Location 数据位置	**DSP-19**	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up. 定义和实施过程、规程和技术措施，以指定和记录数据的物理位置，包括处理或备份数据的任何位置。
Governance, Risk and Compliance - GRC　治理、风险管理和合规		
Governance Program Policy and Procedures 治理计划策略和程序	**GRC-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护由组织领导发起的信息治理计划的策略和规程。至少每年审查和更新策略和规程。
Risk Management Program 风险管理计划	**GRC-02**	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks. 建立一个正式的、记录在案的、由领导层赞助的企业风险管理（ERM）计划，其中包括识别、评估、所有权、处理和接受云安全和隐私风险的策略和规程。
Organizational Policy Reviews 组织策略审查	**GRC-03**	Review all relevant organizational policies and associated procedures at least annually or when a substantial change occurs within the organization. 至少每年或组织内部发生重大变化时，审查所有相关组织策略和相关规程。
Policy Exception Process 策略例外过程	**GRC-04**	Establish and follow an approved exception process as mandated by the governance program whenever a deviation from an established policy occurs. 当发生与既定策略的偏差时，按照治理计划的要求建立并遵循批准的例外过程。

Information Security Program 信息安全计划	**GRC-05**	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM. 制定并实施信息安全计划，包括CCM所有相关领域的计划。
Governance Responsibility Model 治理责任模式	**GRC-06**	Define and document roles and responsibilities for planning, implementing, operating, assessing, and improving governance programs. 定义并记录规划、实施、运营、评估和改进治理计划的角色和职责。
Information System Regulatory Mapping 信息系统监管映射	**GRC-07**	Identify and document all relevant standards, regulations, legal/contractual, and statutory requirements, which are applicable to your organization. 确定并记录所有适用于贵组织的相关标准、法规、法律/合同和法定要求。
Special Interest Groups 特殊利益团体	**GRC-08**	Establish and maintain contact with cloud-related special interest groups and other relevant entities in line with business context. 与云相关的特殊利益团体和其他相关实体建立并保持联系，与业务环境保持一致。
Human Resources - HRS 人力资源		
Background Screening Policy and Procedures 背景调查的策略与规程	**HRS-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties) according to local laws, regulations, ethics, and contractual constraints and proportional to the data classification to be accessed, the business requirements, and acceptable risk. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护背景调查的策略和规程，根据当地的法律、法规、道德和合同约束，针对所有新员工（包括但不限于远程员工，承包商和第三方），根据其可访问的数据分级，业务需求和可接受的风险来决定背景调查的程度。应至少每年检查并更新策略和规程。
Acceptable Use of Technology Policy and Procedures 可接受使用的技术策略与规程	**HRS-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护策略和规程，以定义允许合理使用组织拥有或管理的资产的条件和场合。应至少每年检查并更新策略和规程。
Clean Desk Policy and Procedures 桌面清理的策略与规程	**HRS-03**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures that require unattended workspaces to not have openly visible confidential data. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护相应的策略和规程，要求无人值守的工作场所不存在公开可见的敏感文件。应至少每年检查并更新策略和规程。
Remote and Home Working Policy and Procedures 远程工作的策略与规程	**HRS-04**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect information accessed, processed or stored at remote sites and locations. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护策略和规程，以保护在远程站点和位置下对信息的访问、处理和存储。应至少每年检查并更新策略和规程。
Asset returns 资产归还	**HRS-05**	Establish and document procedures for the return of organization-owned assets by terminated employees. 建立并记录离职员工归还组织拥有资产的规程。
Employment Termination 聘用终止	**HRS-06**	Establish, document, and communicate to all personnel the procedures outlining the roles and responsibilities concerning changes in employment. 建立、记录并向所有人员传达规程，概述与聘用变更相关的角色和责任。
Employment Agreement Process 聘用协议过程	**HRS-07**	Employees sign the employee agreement prior to being granted access to organizational information systems, resources and assets. 员工在被授予访问组织信息系统，资源和资产的权限之前应签署员工协议。
Employment Agreement Content 聘用协议内容	**HRS-08**	The organization includes within the employment agreements provisions and/or terms for adherence to established information governance and security policies. 组织在雇佣协议中包含遵守既定信息治理和安全策略的协议或条款。
Personnel Roles and Responsibilities 人员角色和职责	**HRS-09**	Document and communicate roles and responsibilities of employees, as they relate to information assets and security. 记录并传达员工的角色和职责，因为它们与信息资产和安全有关。
Non-Disclosure Agreements 保密协议	**HRS-10**	Identify, document, and review, at planned intervals, requirements for non-disclosure/confidentiality agreements reflecting the organization's needs for the protection of data and operational details. 定期确定、记录和评审对保密/保密协议的要求，这些要求反映了组织对数据和执行细节的保护需求。

Security Awareness Training 信息安全意识培训	**HRS-11**	Establish, document, approve, communicate, apply, evaluate and maintain a security awareness training program for all employees of the organization and provide regular training updates. 为组织的所有员工建立、记录、批准、沟通、应用、评估和维护信息安全意识培训计划，并提供定期的培训更新。
Personal and Sensitive Data Awareness and Training 个人与敏感信息的意识与培训	**HRS-12**	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization. 为所有有权限访问敏感组织和个人信息数据的员工提供适当的安全意识培训，并定期更新与他们相对于组织的专业职能有关的组织规程、过程和策略。
Compliance User Responsibility 用户合规责任	**HRS-13**	Make employees aware of their roles and responsibilities for maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. 使员工了解他们的角色和职责，以保持对既定策略和规程以及适用的法律，法规或监管合规性义务的认识和遵守。

Identity & Access Management - IAM 身份与访问控制

Identity and Access Management Policy and Procedures 身份与访问控制的策略与规程	**IAM-01**	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、实施、应用、评估和维护身份和访问控制的策略和规程。应至少每年检查并更新该策略和规程。
Strong Password Policy and Procedures 强密码的策略与规程	**IAM-02**	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、实施、应用、评估和维护强密码策略和规程。应至少每年检查并更新该策略和规程。
Identity Inventory 身份清单	**IAM-03**	Manage, store, and review the information of system identities, and level of access. 管理，存储和评审系统的身份信息和访问级别。
Separation of Duties 职责分离	**IAM-04**	Employ the separation of duties principle when implementing information system access. 实施信息系统访问时，采用职责分离原则。
Least Privilege 最小权限	**IAM-05**	Employ the least privilege principle when implementing information system access. 实施信息系统访问时，采用最小权限原则。
User Access Provisioning 用户访问授权	**IAM-06**	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets. 定义并实施用户访问权限配置过程，该过程授权，记录和传达对数据和资产的访问权限更改。
User Access Changes and Revocation 用户访问变更与撤销	**IAM-07**	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner in order to effectively adopt and communicate identity and access management policies. 及时撤销或更改岗位变更/离职人员的访问权限或变更系统身份认证，以有效地适应和传达身份和访问控制策略。
User Access Review 用户访问评审	**IAM-08**	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance. 定期检查并重新验证用户访问权限，以满足最小权限和职责分离原则检查的频率应与组织风险承受能力相称。
Segregation of Privileged Access Roles 特权访问角色的隔离	**IAM-09**	Define, implement and evaluate processes, procedures and technical measures for the segregation of privileged access roles such that administrative access to data, encryption and key management capabilities and logging capabilities are distinct and separated. 定义、实施和评估用于隔离特权访问角色的过程、规程和技术措施，以使对特权访问角色、数据的管理访问、加密和密钥管理功能、以及日志记录功能进行区别和隔离。
Management of Privileged Access Roles 特权访问角色的管理	**IAM-10**	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period, and implement procedures to prevent the culmination of segregated privileged access. 定义并实施访问过程，以确保在有限的时间段内授予特权访问角色和权限，并实施规程以防止隔离的特权访问出现峰值异常。
CSCs Approval for Agreed Privileged Access Roles 特权访问角色的商业批准	**IAM-11**	Define, implement and evaluate processes and procedures for customers to participate, where applicable, in the granting of access for agreed, high risk (as defined by the organizational risk assessment) privileged access roles. 组织在授权高风险（由组织风险评估定义）特权访问角色时，适当情况下，可由客户联合参与授权，应定义、实施和评估相应的过程和规程。

Safeguard Logs Integrity 保障日志完整性	**IAM-12**	Define, implement and evaluate processes, procedures and technical measures to ensure the logging infrastructure is read-only for all with write access, including privileged access roles, and that the ability to disable it is controlled through a procedure that ensures the segregation of duties and break glass procedures. 定义、实施和评估过程，规程和技术措施，以确保所有具有写入访问权限的角色（包括特权访问角色）对日志记录基础设施都是只读的，并通过一个确保实现职责分离和必要时可临时授予访问权限的管理规程来禁用其控制权限。
Uniquely Identifiable Users 唯一可识别用户	**IAM-13**	Define, implement and evaluate processes, procedures and technical measures that ensure users are identifiable through unique IDs or which can associate individuals to the usage of user IDs. 定义、实施和评估过程，规程和技术措施，以确保可以通过唯一ID识别用户，或者可以将个人与用户ID的使用相关联。
Strong Authentication 强鉴别	**IAM-14**	Define, implement and evaluate processes, procedures and technical measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities. 定义、实施和评估过程、规程和技术措施，以对系统，应用程序和数据资产进行鉴别访问，包括对至少特权用户和敏感数据访问的多因素认证、采用数字证书或替代证书等，以使系统的身份控制达到与系统相应的安全级别。
Passwords Management 密码管理	**IAM-15**	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords. 定义、实施和评估用于密码安全管理的过程、规程和技术措施。
Authorization Mechanisms 认证机制	**IAM-16**	Define, implement and evaluate processes, procedures and technical measures to verify access to data and system functions is authorized. 定义、实施和评估过程、规程和技术措施，以验证是否有权访问数据和系统功能。
Interoperability & Portability - IPY 互操作性与可移植性		
Interoperability and Portability Policy and Procedures 互操作性与可移植性策略与规程	**IPY-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for interoperability and portability including requirements for: a. Communications between application interfaces b. Information processing interoperability c. Application development portability d. Information/Data exchange, usage, portability, integrity, and persistence Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护关于互操作性和可移植性的策略和规程，并包括以下要求： a. 应用程序接口之间的通信 b. 信息处理的互操作性 c. 应用程序开发的可移植性 d. 信息/数据的交换、使用、完整性和持久性 至少每年一次对策略和规程进行审查并更新。
Application Interface Availability 应用程序接口可用性	**IPY-02**	Provide application interface(s) to CSCs so that they programmatically retrieve their data to enable interoperability and portability. 为云服务客户提供应用程序接口，使他们可以通过编程方式检索他们的数据，从而实现互操作性和可移植性。
Secure Interoperability and Portability Management 保护互操作性与可移植性管理	**IPY-03**	Implement cryptographically secure and standardized network protocols for the management, import and export of data. 为数据的管理、导入和导出实施密码学安全和标准化的网络协议。

Data Portability Contractual Obligations 数据可移植性的合同义务	**IPY-04**	Agreements must include provisions specifying CSCs access to data upon contract termination and will include: a. Data format b. Length of time the data will be stored c. Scope of the data retained and made available to the CSCs d. Data deletion policy 协议必须包括相关条款，规定云服务客户在合同终止时可以访问数据，并包括: a. 数据格式。 b. 数据存储的时间长度 c. 保留和提供给云服务客户的数据的范围 d. 数据删除策略
Infrastructure & Virtualization Security - IVS 基础设施与虚拟化安全		
Infrastructure and Virtualization Security Policy and Procedures 基础设施与虚拟化安全策略与规程	**IVS-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护关于基础设施和虚拟化安全的策略与规程并至少每年一次进行审查和更新。
Capacity and Resource Planning 容量与资源计划	**IVS-02**	Plan and monitor the availability, quality, and adequate capacity of resources in order to deliver the required system performance as determined by the business. 计划和监控资源的可用性、质量和充分的容量，以交付业务所需的系统性能。
Network Security 网络安全	**IVS-03**	Monitor, encrypt and restrict communications between environments to only authenticated and authorized connections, as justified by the business. Review these configurations at least annually, and support them by a documented justification of all allowed services, protocols, ports, and compensating controls. 根据业务需要，监控、加密和限制环境之间的通信，仅允许经过鉴别与授权的连接。 至少每年审查一次这些配置，并通过所有允许的服务，协议，端口和补偿控制的书面证明为它们提供支持。
OS Hardening and Base Controls 操作系统加固与基线控制	**IVS-04**	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline. 根据其对应的最佳实践，对主机(host)和客机(guest)操作系统、虚拟机监控器(Hypervisor)或基础设施控制平面进行加固。并将其作为安全基线的一部分，得到技术控制措施的支持。
Production and Non-Production Environments 生产与非生产环境	**IVS-05**	Separate production and non-production environments. 隔离生产和非生产环境。
Segmentation and Segregation 分区与隔离	**IVS-06**	Design, develop, deploy and configure applications and infrastructures such that CSP and CSC (tenant) user access and intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants. 设计、开发、部署和配置应用程序和基础设施，使云服务提供商和云服务客户（租户）的用户访问、租户的内部访问均得到适当的分区和隔离，监控及限制其他租户访问。
Migration to Cloud Environments 迁移到云环境	**IVS-07**	Use secure and encrypted communication channels when migrating servers, services, applications, or data to cloud environments. Such channels must include only up-to-date and approved protocols. 在将服务器、服务、应用程序或数据迁移到云环境时，请使用安全加密的通信通道。此类通道必须仅包括最新的和获批准的协议。
Network Architecture Documentation 网络架构文档	**IVS-08**	Identify and document high-risk environments. 识别和记录高风险环境。
Network Defense 网络防御	**IVS-09**	Define, implement and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks. 对过程、规程和深度防御技术进行定义、实施和评估，以保护、检测并及时响应基于网络的攻击。
Logging and Monitoring - LOG 日志记录与监控		
Logging and Monitoring Policy and Procedures 日志记录与监控策略与规程	**LOG-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护关于记录与监控的策略和规程，并至少每年一次对策略和规程进行审查和更新。
Audit Logs Protection 审计日志保护	**LOG-02**	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs. 定义、实施相关过程、规程和技术措施，并进行评估，以确保审计日志的安全和保留。

Security Monitoring and Alerting 安全监控与告警	**LOG-03**	Identify and monitor security-related events within applications and the underlying infrastructure. Define and implement a system to generate alerts to responsible stakeholders based on such events and corresponding metrics. 对应用程序和底层基础设施中与安全相关的事态进行识别和监控。定义并实施一个系统，根据相关事态和指标向负责的相关方发出告警。
Audit Logs Access and Accountability 审计日志访问与责任	**LOG-04**	Restrict audit logs access to authorized personnel and maintain records that provide unique access accountability. 仅允许获得授权的人员访问审计日志，并维护可提供唯一访问可核查性的记录。
Audit Logs Monitoring and Response 审计日志监控与响应	**LOG-05**	Monitor security audit logs to detect activity outside of typical or expected patterns. Establish and follow a defined process to review and take appropriate and timely actions on detected anomalies. 监控安全审计日志，以检测典型或预期模式之外的活动。建立并遵循预先定义的过程，对发现的异常进行审查，并及时采取适当的措施。
Clock Synchronization 时钟同步	**LOG-06**	Use a reliable time source across all relevant information processing systems. 在所有相关的信息处理系统中使用可靠的时间源。
Logging Scope 日志记录范围	**LOG-07**	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment. 确定并记录哪些信息元/数据系统事态应被日志记录，并予以实施。至少每年一次，或在威胁环境发生变化时，对该范围进行审查和更新。
Log Records 日志记录	**LOG-08**	Generate audit records containing relevant security information. 生成包含相关安全信息的审计记录。
Log Protection 日志保护	**LOG-09**	The information system protects audit records from unauthorized access, modification, and deletion. 信息系统保护审计记录免受非授权的访问、修改和删除。
Encryption Monitoring and Reporting 加密监控与报告	**LOG-10**	Establish and maintain a monitoring and internal reporting capability over the operations of cryptographic, encryption and key management policies, processes, procedures, and controls. 建立并维护关于对密码操作、加密和密钥管理的策略、过程、规程和控制进行监控和内部报告的能力。
Transaction/Activity Logging 交易/活动日志	**LOG-11**	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys. 记录和监控密钥生命周期管理事态，以支持对加密密钥的使用情况进行审计和报告。
Access Control Logs 访问控制日志	**LOG-12**	Monitor and log physical access using an auditable access control system. 使用可审计的访问控制系统对物理访问进行监控和记录。
Failures and Anomalies Reporting 故障与异常报告	**LOG-13**	Define, implement and evaluate processes, procedures and technical measures for the reporting of anomalies and failures of the monitoring system and provide immediate notification to the accountable party. 定义、实施和评估对监控系统的异常和故障进行报告的过程、规程和技术措施，并立即通知责任方。
Security Incident Management, E-Discovery, & Cloud Forensics - SEF 安全事件管理，电子发现及云取证		
Security Incident Management Policy and Procedures 安全事件管理策略与规程	**SEF-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护安全事件管理、电子发现和云取证的策略和规程。至少每年审核并更新该策略和规程。
Service Management Policy and Procedures 服务管理策略与规程	**SEF-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the timely management of security incidents. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护相关策略和规程, 以确保安全事件及时管理。至少每年审核并更新该策略和规程。
Incident Response Plans 事件响应计划	**SEF-03**	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted. 建立、记录、批准、沟通、应用、评估和维护安全事件响应计划，包括但不限于：相关内部部门、受影响的客户（租户）和其他可能受影响的关键业务关系（比如供应链）。

Incident Response Testing 事件响应测试	**SEF-04**	Test and update as necessary incident response plans at planned intervals or upon significant organizational or environmental changes for effectiveness. 根据计划的频率，或者在发生重大组织或环境变更时测试安全事件响应计划的有效性并按需更新该计划。
Incident Response Metrics 事件响应指标	**SEF-05**	Establish and monitor information security incident metrics. 建立和监控信息安全事件指标。
Event Triage Processes 事态分类过程	**SEF-06**	Define, implement and evaluate processes, procedures and technical measures supporting business processes to triage security-related events. 定义、实施以及评估相关过程、规程以及技术手段以支持业务流程对安全相关的事态进行分类。
Security Breach Notification 安全违规通知	**SEF-07**	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations. 定义并实施与安全违规通知相关的过程、规程以及技术手段。根据相关的SLA，法律法规要求来报告安全事故以及假定安全违规(assumed security breaches)，包括供应链相关的安全违规。
Points of Contact Maintenance 联络人维护	**SEF-08**	Maintain points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities. 维护相关法律法规监管、国家和当地司法机关的联络人清单。
Supply Chain Management, Transparency, and Accountability - STA 供应链管理，透明性和可核查性		
SSRM Policy and Procedures 共享安全责任模型策略与规程	**STA-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for the application of the Shared Security Responsibility Model (SSRM) within the organization. Review and update the policies and procedures at least annually. 建立、记录、批准、沟通、应用、评估和维护在组织内应用共享安全责任模型（SSRM）的策略和规程。至少每年评审和更新策略和规程。
SSRM Supply Chain 共享安全责任模型供应链	**STA-02**	Apply, document, implement and manage the SSRM throughout the supply chain for the cloud service offering. 在整个云服务供应链中应用、记录、实施和管理共享安全责任模型（SSRM）。
SSRM Guidance 共享安全责任模型指南	**STA-03**	Provide SSRM Guidance to the CSC detailing information about the SSRM applicability throughout the supply chain. 向CSC提供SSRM指南，详细说明SSRM在整个供应链中的适用性信息。
SSRM Control Ownership 共享安全责任模型控制所有权	**STA-04**	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering. 根据云服务产品的SSRM描述所有CSA、CCM控件的共享所有权和适用性。
SSRM Documentation Review 共享安全责任模型文档审阅	**STA-05**	Review and validate SSRM documentation for all cloud services offerings the organization uses. 评审和验证组织使用的所有云服务产品的SSRM文档。
SSRM Control Implementation 共享安全责任模型控制实施	**STA-06**	Implement, operate, and audit or assess the portions of the SSRM which the organization is responsible for. 实施、操作、审计或评估组织负责的SSRM部分。
Supply Chain Inventory 供应链清单	**STA-07**	Develop and maintain an inventory of all supply chain relationships. 开发并维护所有供应链关系的清单。
Supply Chain Risk Management 供应链风险管理	**STA-08**	CSPs periodically review risk factors associated with all organizations within their supply chain. CSP（云服务提供商）定期评审供应链内部所有组织的风险因素。

Primary Service and Contractual Agreement 基本服务及合同协议	**STA-09**	Service agreements between CSPs and CSCs (tenants) must incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope, characteristics and location of business relationship and services offered • Information security requirements (including SSRM) • Change management process • Logging and monitoring capability • Incident management and communication procedures • Right to audit and third party assessment • Service termination • Interoperability and portability requirements • Data privacy CSP（云服务提供商）与CSC（云服务客户）之间的服务协议必须至少包含以下相互同意的规定和/或条款： •业务关系和提供服务的范围、特点和位置 •信息安全要求（包括SSRM） •变更管理流程 •记录和监视能力 •事件管理和沟通规程 •审计权和第三方评估权 •服务终止 •互操作性和可移植性要求 •数据隐私
Supply Chain Agreement Review 供应链协议审阅	**STA-10**	Review supply chain agreements between CSPs and CSCs at least annually. 至少每年评审CSP（云服务提供商）和CSC（云服务客户）之间的供应链协议。
Internal Compliance Testing 内部合规评测	**STA-11**	Define and implement a process for conducting internal assessments to confirm conformance and effectiveness of standards, policies, procedures, and service level agreement activities at least annually. 至少每年规定并实施一个内部评估流程，以确认标准、策略、规程和服务级别协议活动的合规性和有效性。
Supply Chain Service Agreement Compliance 供应链服务协议合规	**STA-12**	Implement policies requiring all CSPs throughout the supply chain to comply with information security, confidentiality, access control, privacy, audit, personnel policy and service level requirements and standards. 实施策略要求整个供应链的所有CSP（云服务提供商）遵守信息安全、保密、访问控制、隐私、审计、人事策略、和服务级别要求和标准。
Supply Chain Governance Review 供应链治理审阅	**STA-13**	Periodically review the organization's supply chain partners' IT governance policies and procedures. 定期评审组织的供应链合作伙伴的IT治理策略和规程。
Supply Chain Data Security Assessment 供应链数据安全评估	**STA-14**	Define and implement a process for conducting security assessments periodically for all organizations within the supply chain. 定期规定并实施一个对供应链内部所有组织进行安全评估的过程。
Threat & Vulnerability Management - TVM 威胁、脆弱性管理		
Threat and Vulnerability Management Policy and Procedures 威胁、脆弱性管理策略及规程	**TVM-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, in order to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually. 建立、文档化、批准、沟通、应用、评估和维护策略和规程，以识别、报告和设置脆弱性解决的优先级，从而保护系统免受漏洞攻击。至少每年审查和更新策略和规程。
Malware Protection Policy and Procedures 恶意软件保护策略和规程	**TVM-02**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually. 建立、文档化、批准、沟通、应用、评估和维护策略和规程，以防范受管理资产被恶意软件侵害。至少每年审查和更新策略和规程。
Vulnerability Remediation Schedule 脆弱性补救程序	**TVM-03**	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk. 定义、实施和评估相关的过程、规程和技术措施，基于已识别的风险，对脆弱性识别实施程序和应急响应。

Detection Updates 检测更新	**TVM-04**	Define, implement and evaluate processes, procedures and technical measures to update detection tools, threat signatures, and indicators of compromise on a weekly, or more frequent basis. 每周或更频繁地定义、实施过程、规程和技术措施，更新检测工具、威胁特征和攻击指标（IOC）指标。
External Library Vulnerabilities 外部库脆弱性	**TVM-05**	Define, implement and evaluate processes, procedures and technical measures to identify updates for applications which use third party or open source libraries according to the organization's vulnerability management policy. 定义、实施和评估过程、规程和技术措施，根据组织的脆弱性管理策略，为使用第三方或开源库的应用程序识别更新。
Penetration Testing 渗透测试	**TVM-06**	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties. 定义、实施和评估过程、规程和技术措施，定期开展由独立第三方渗透测试。
Vulnerability Identification 脆弱性识别	**TVM-07**	Define, implement and evaluate processes, procedures and technical measures for the detection of vulnerabilities on organizationally managed assets at least monthly. 定义、实施和评估过程、规程和技术措施，至少每月检测组织管理资产的脆弱性。
Vulnerability Prioritization 脆弱性优先级	**TVM-08**	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework. 使用基于风险的模型以及业界公认的框架，有效地确定脆弱性补救的优先级。
Vulnerability Management Reporting 脆弱性汇报管理	**TVM-09**	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification. 定义并实施跟踪和报告脆弱性识别和补救活动的过程，包括通知利益相关方。
Vulnerability Management Metrics 脆弱性管理指标	**TVM-10**	Establish, monitor and report metrics for vulnerability identification and remediation at defined intervals. 在规定的时间间隔内，建立、监控和报告脆弱性识别和补救的指标。

Universal Endpoint Management - UEM 统一终端管理

Endpoint Devices Policy and Procedures 端点设备策略和规程	**UEM-01**	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually. 为所有终端建立、文档化、批准、沟通、应用、评估和维护策略和规程。至少每年审查和更新策略和规程。
Application and Service Approval 应用和服务批准	**UEM-02**	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data. 在访问或存储组织管理的数据时，定义、文档化、应用和评估可供终端使用的已批准服务、应用程序和应用程序源（商店）的列表。
Compatibility 兼容性	**UEM-03**	Define and implement a process for the validation of the endpoint device's compatibility with operating systems and applications. 定义并实现验证终端设备的操作系统和应用程序兼容性的过程。
Endpoint Inventory 终端清单	**UEM-04**	Maintain an inventory of all endpoints used to store and access company data. 维护用于存储和访问公司数据的所有终端设备的清单。
Endpoint Management 终端管理	**UEM-05**	Define, implement and evaluate processes, procedures and technical measures to enforce policies and controls for all endpoints permitted to access systems and/or store, transmit, or process organizational data. 定义、实施和评估过程、规程和技术措施，以便对允许访问系统和/或存储、传输或处理组织数据的所有终端实施策略和控制。
Automatic Lock Screen 自动锁屏	**UEM-06**	Configure all relevant interactive-use endpoints to require an automatic lock screen. 配置所有交互式终端，要求自动锁定屏幕。
Operating Systems 操作系统	**UEM-07**	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes. 通过公司的变更管理过程，管理终端操作系统、修补程序级别和/或应用程序的更改。
Storage Encryption 存储加密	**UEM-08**	Protect information from unauthorized disclosure on managed endpoint devices with storage encryption. 使用存储加密保护终端设备上的信息不被未经授权的泄露。
Anti-Malware Detection and Prevention 反恶意软件检测与防范	**UEM-09**	Configure managed endpoints with anti-malware detection and prevention technology and services. 使用反恶意软件检测和预防技术和及服务配置受管理终端。

Software Firewall 软件防火墙	**UEM-10**	Configure managed endpoints with properly configured software firewalls. 使用正确配置的软件防火墙配置受管理终端。
Data Loss Prevention 数据丢失防护	**UEM-11**	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment. 根据风险评估，使用数据丢失预防数据防泄漏（DLP）技术和规则配置受管理终端。
Remote Locate 远程定位	**UEM-12**	Enable remote geo-location capabilities for all managed mobile endpoints. 为所有受管理移动终端启用远程地理位置功能。
Remote Wipe 远程擦除	**UEM-13**	Define, implement and evaluate processes, procedures and technical measures to enable the deletion of company data remotely on managed endpoint devices. 定义、实施和评估过程、规程和技术措施，以便能够远程删除受管理终端设备上的公司数据。
Third-Party Endpoint Security Posture 第三方终端安全态势	**UEM-14**	Define, implement and evaluate processes, procedures and technical and/or contractual measures to maintain proper security of third-party endpoints with access to organizational assets. 定义、实施和评估过程、规程以及技术和/或合同措施，以维护访问组织资产的第三方终端的适当安全。

End of Standard