云安全控制矩阵 CCM　中英文版

Control 控制措施	CCM V3.0 Control ID	Updated Control Specification 更新的控制措施规范
		Application & Interface Security 应用程序和接口安全
Application Security 应用程序安全	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.应按照行业的主流标准（例如针对 WEB 应用的 OWASP），并遵守适用的法律、法规或其它监管合规要求来设计、开发、部署并测试相关应用与程序的 API。
Customer Access Requirements 客户访问要求	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.应在赋予客户对数据、资产和信息系统的访问权之前，确定客户访问的安全、合同和监管的要求。
Data Integrity 数据完整性	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.应对应用程序接口和数据库的数据输入和输出进行常规的完整性校验（即：一致性和编辑检查），以防止人为或系统性的处理错误、数据损坏或误用。
Data Security / Integrity 安全/完整性	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction.应建立并保持策略和规程，以支持跨越多个系统接口、司法管辖区和职能部门的数据的安全（包括保密性、完整性和可用性），防止对数据不正当泄露、修改和破坏。

Audit Assurance & Compliance 审计保障与合规性

Audit Planning 审计策划	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.应开发并维护审计计划以处理业务流程中断。审计计划应关注于对安全运营实施有效性的评审。任何审计活动应在执行之前获得许可。
Independent Audits 独立审计	AAC-02	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.应至少每年实施一次独立的评审和评估以确保组织处理了在建立策略、标准、规程和法律符合性方面的不符合情况。
Information System Regulatory Mapping 信息系统合规映射	AAC-03	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.组织应创建并维护一个用以搜集和业务需求相关的标准、法律、法规和强制性要求的控制框架。控制框架应至少每年进行评审以确保可能影响业务流程的变化在框架中得到体现。

Business Continuity Management & Operational Resilience 业务连续性管理与运营恢复

Business Continuity Planning 业务连续性的策划	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. 应以文件化形式建立并采用一个关于业务连续性计划以及计划的开发所需的一致性统一框架，以确保所有的业务连续性计划在测试、维护之前得以完成，并符合信息安全要求。 Requirements for business continuity plans include the following:业务连续性计划的要求包括以下方面： • Defined purpose and scope, aligned with relevant dependencies 明确的目的和范围，并与相关依存条件一致 • Accessible to and understood by those who will use them 可被使用者获取并理解 • Owned by a named person(s) who is responsible for their review, update, and approval 评审、更新和批准的职责明确到人 • Defined lines of communication, roles, and responsibilities 明确的沟通、角色和责任名单 • Detailed recovery procedures, manual work-around, and reference information 详细的恢复程序、手动应急措施和参考信息 • Method for plan invocation 计划调用的方法

Business Continuity Testing 业务连续性的测试	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.业务连续性和安全事件响应计划应按计划的周期或在组织和环境发生重大变化时进行测试。事件响应计划应包括受到事件影响，且代表关键内部供应链业务流程的客户（租户）和其他业务关系。
Datacenter Utilities / Environmental Conditions 数据中心设施/环境状况	BCR-03	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications,and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.应按计划的时间间隔对数据基础设施服务和环境条件（如：水、电、温湿度控制、通信以及因特网连接）的持续有效性进行保障、监控、维护和测试，保证其免于受到非授权的窃取或破坏，并设计在面临计划内和计划外中断事态时的自动化故障转移或其他方面的冗余机制。
Documentation 文档化	BCR-03	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:应确保信息系统文档（如：管理员指南、用户指南、架构图）对于授权人员是可获取的，以确保： • Configuring, installing, and operating the information system 配置、安装和运行信息系统； • Effectively using the system's security features 有效使用系统的安全功能。
Environmental Risks 环境风险	BCR-05	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.应预测、设计并应用物理防护措施以抵御自然灾害和蓄意攻击，如火灾、洪水、大气放电、太阳磁暴、大风、地震、海啸、爆炸、核事故、火山活动、生物危机、内乱、泥石流、构造活动和其他形式的自然或人为灾难。
Equipment Location 设备放置	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.为减少环境威胁和危害，以及未授权访问的风险，设备应远离高危环境，并将冗余设备部署在合适的距离。

Equipment Maintenance 设备维护	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.应建立设备维护的策略和规程，并实施支持性业务流程和技术手段，以确保操作和支持人员的持续性和可用性。
Equipment Power Failures 设备电力失效	BCR-08	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment 应根据基于具体地理位置的业务影响评估的结果落实保护措施，以应对自然和人为威胁。
Impact Analysis 影响性分析	BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following:应定义并记录任何可确定中断对组织（云供应商、云客户）带来的影响的方法，该方法须包含以下内容： • Identify critical products and services 识别关键产品和服务； • Identify all dependencies, including processes, applications, business partners, and third party service providers 识别所有依赖关系，包括流程、应用系统、商业伙伴和第三方服务提供商； • Understand threats to critical products and services 理解关键产品和服务面临的威胁； • Determine impacts resulting from planned or unplanned disruptions and how these vary over time 确定计划内或计划外的中断导致的影响，以及这些影响如何随时间而变化； • Establish the maximum tolerable period for disruption 确定最长可容忍中断时间（MTPD）； • Establish priorities for recovery 确定恢复优先级； • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption 根据关键产品和服务的最长可容忍中断时间（MTPD）确定恢复时间目标（RTO）； • Estimate the resources required for resumption 确定恢复至正常状态所需的资源。
Policy 策略	BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v3 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.应建立适宜的 IT 治理和服务管理相关的策略和规程，并基于行业可接受标准（如 ITIL v3 和 COBIT 5）实施支持性业务流程和技术手段，以保证适宜的策划、交付和支持组织的 IT 能力用于支持业务职能、员工和/或客户。同时，策略和规程应包括确定的角色和职责，并辅以定期的员工培训。

Retention Policy 保存策略	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.应建立定义了所有关键资产保存期限的策略和规程，并实施支持性业务流程和技术手段。每一项策略、规程以及适用的法律、法规和合规性义务应得到遵从。备份与恢复措施也应该作为 BCP 的一个组成部分，并通过有效性测试。

Change Control & Configuration Management 变更控制和配置管理

New Development / Acquisition 新开发/获取	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.应建立策略和规程，并实施支持性业务流程和技术手段，以确保开发和/或获取新数据、物理或虚拟应用、基础网络设施和系统组件、或任何公司的、运营的和/或数据中心的设施时，得到组织的业务领导或其他负责的业务角色或部门的预授权。
Outsourced Development 外包开发	CCC-02	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).外部业务伙伴应和组织内部开发者一样遵守相同的变更、发布和测试策略和规程（如：ITIL 服务管理流程）。
Quality Testing 质量测试	CCC-03	Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.组织应遵循已定义的质量变更控制和测试流程（如：ITIL 服务管理），基于已建立的关注于系统可用性、保密性和系统/服务完整性的基线、测试和发布标准。
Unauthorized Software Installations 非授权软件安装	CCC-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.应建立策略和规程，并实施支持性业务流程和技术手段，以限制在组织拥有或管理的用户终端设备（如：配发的工作站、笔记本电脑和移动设备）、IT 基础网络设施和系统组件上安装非授权软件。

Production Changes 生产变更	CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to:应建立策略和规程以管理与变更实施相关的风险： • business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations 对关键业务或客户（租户）产生影响（物理或虚拟）的应用程序，及系统间接口（API）的设计和配置； • infrastructure network and systems components 基础设施网络和系统组件； Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.应实施技术手段来为所有直接与已登记的变更请求、关键业务或客户（租户）相关的变更提供保证，并/或在部署前按协议（SLA）要求获得客户（租户）授权。
Data Security & Information Lifecycle Management　数据安全与信息生命周期管理		
Classification 分类	DSI-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.应由数据责任人基于数据类型、数据值和对于组织的敏感程度、关键程度，对数据和包含数据的对象进行分类。
Data Inventory / Flows 数据目录/数据流	DSI-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.应建立策略和规程，并实施支持性业务流程和技术手段，对永久性或临时性留存在分布于物理和虚拟区域的服务中的应用程序、基础网络和系统组件的，和/或其他第三方分享的数据进行归档、记录，以及数据流的维护，以确定任何有关法律法规或 SLA 符合性影响，并确定其他和数据相关的业务风险。基于以上的要求，提供商应告知客户（租户）关于合规的影响和风险，特别是当客户数据作为服务的一部分时。

eCommerce Transactions 电子商务交易	DSI-03	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.穿越公共网络的电子商务（e-commerce）数据应被适当的分类和保护，以防止遭受欺诈、非授权披露或修改，避免合同纠纷和数据破坏。
Handling / Labeling / Security Policy 处理/标示/安全策略	DSI-04	Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.应针对数据及包含数据的对象，建立有关数据标识、处理和数据安全的策略和规程。对作为聚合数据容器的对象实行标签继承机制。
Non-Production Data 非生产数据	DSI-05	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.应防止生产数据被复制或使用于非生产环境。任何在非生产环境中使用客户数据的行为应该经该客户明确许可并记录，同时必须符合敏感数据擦除相关的法律法规要求。
Ownership / Stewardship 责任人/管理者	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.所有数据的管理工作应被定义，并以文件化形式定义和传达被分配的职责。
Secure Disposal 安全处置	DSI-07	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.应建立策略和规程，并实施支持性业务流程和技术手段，以安全处置并完全移除所有存储介质中的数据，确保数据没有被任何计算机取证方式所恢复。

Datacenter Security　数据中心安全		
Asset Management 资产管理	DCS-01	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.必须按照对业务的关键程度、服务级别期望和运营连续性的要求对资产进行分类。应针对所有场所和区域的资产以及它们的用途，维护一份完整的关键业务资产清单，保持定期的更新，并按照定义的角色和职责来分配责任人。
Controlled Access Points 可控访问点	DCS-02	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.应实施物理安全边界（如：栅栏、墙、障碍物、保安、门、电子检测、物理认证机制、前台、安全巡逻）来保护敏感数据和信息系统。
Equipment Identification 设备识别	DCS-03	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location. 应使用自动设备识别作为连接认证授权的方法。位置感知技术可被用于根据已知设备位置来验证连接认证的完整性。
Off-Site Authorization 场外授权	DCS-04	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.硬件、软件或数据在搬移或传输到场外前必须经过授权。
Off-Site Equipment 场外设备	DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.应建立策略和规程，以保证组织场所以外的设备（按资产类型），通过使信息不可恢复的擦除方案或破坏流程进行了安全处置。应通过对驱动器完整覆写的擦除方式，来确保擦除的驱动器可以回归资源池以供再次使用和部署，或使数据被安全存储直至被破坏。

Policy 策略	DCS-06	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.应建立策略和规程，并实施支持性业务流程，以在存有敏感信息的办公室、房间、设施以及安全区域内维护一个安全的工作环境。
Secure Area Authorization 安全区域授权	DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.安全区域的出入应采用物理访问控制机制加以限制和监视，以确保只有经过授权的人员可以访问。
Unauthorized Persons Entry 非授权人员进入	DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.出入区域，如服务区和其他非授权人员可能进入的区域，应被监视、控制并与数据存储和处理设施相隔离（如可能），以防止未经授权的数据破坏、损害和损失。
User Access 用户访问	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.应限制用户和支持人员对信息资产和职能部门的物理访问。
Encryption & Key Management 加密与密钥管理		
Entitlement 权限	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.密钥必须具备可识别的所有者（将密钥与身份绑定），并建立密钥管理策略。
Key Generation 密钥生成	EKM-02	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.应建立策略和规程，以管理服务加密系统中的密钥（如：从密钥生成到撤销和更换的全生命周期，公钥架构、加密协议设计和算法使用，安全密钥生成的访问控制，以及加密数据或会话的交换和隔离存储）。按要求，提供商应通知客户（租户）有关密码系统的变更，特别是当客户（租户）的数据作为服务的一部分，和/或客户（租户）共同承担控制措施实施责任时。

Sensitive Data Protection 敏感数据保护	EKM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.使用加密协议时应建立策略和规程，并实施支持性业务流程和技术手段，按照适用的法律、法规和合规性义务，以保护敏感数据的存储（如文件服务器、数据库、终端用户工作站）、使用（内存中数据）、传输（如系统交互、跨越公共网络和电子消息）。
Storage and Access 存储和访问	EKM-04	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.应要求使用开放、可验证格式和标准算法（例如，AES-256）对平台和数据进行适当加密。密钥不应被存储在云端（即：存在争议的云服务提供商），而是由云用户或可信的密钥管理服务商维护。密钥管理和密钥使用应做到职责分离。
Governance and Risk Management 治理与风险管理		
Baseline Requirements 基线要求	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.应对应用软件、基础系统和网络组件建立安全基线要求，涵盖自主开发或采购的、组织拥有或管理的、物理或虚拟的应用、基础架构系统和网络组件，使其遵循适用的法律法规和合规性义务。标准基线配置的偏差必须在部署、配置或使用前按照变更管理策略和规程执行授权。安全基线要求应至少每年重新评估一次，除非已授权了另一个基于业务需求的评估频率。

Data Focus Risk Assessments 关注数据的风险评估	GRM-02	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:应按计划的时间隔执行与数据治理要求相关的风险评估，并考虑以下方面： • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure 意识到敏感数据会在应用程序、数据库、服务器和网络架构中被存储和传输到哪些地方； • Compliance with defined retention periods and end-of-life disposal requirements 符合定义的保留期和废弃处置的要求 • Data classification and protection from unauthorized use, access, loss, destruction, and falsification 为防止未授权使用、访问、丢失、损毁和伪造，而进行的数据分类和保护。
Management Oversight 管理者监督	GRM-03	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.管理者负责保持其管辖范围相关的安全策略、规程和标准的意识知晓与合规遵从。
Management Program 管理程序	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business:应开发文件化的信息安全管理方案（ISMP）并得到批准和实施，该方案包括管理、技术和物理的安全保护，使资产和数据免受丢失、误用、非授权访问、泄露、修改和破坏。根据其与业务特性的相关程度，安全方案应包括但不限于以下内容： • Risk management 风险管理 • Security policy 安全策略 • Organization of information security 信息安全组织 • Asset management 资产管理 • Human resources security 人力资源安全 • Physical and environmental security 物理和环境安全 • Communications and operations management 通信和操作管理 • Access control 访问控制 • Information systems acquisition, development, and maintenance 信息系统获取、开发和维护。
Management Support/Involvement 管理层支持/参与	GRM-05	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.各级管理层应通过明确的、文档化的指引和承诺，采取正式的行动来支持信息安全，并确保行动已被分配。

Policy 策略	GRM-06	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.应建立信息安全政策和程序，并使之可供所有受影响的人员和外部业务关系随时评审。信息安全政策必须由组织的业务领导（或其他负责的业务角色或部门）授权，获得业务战略计划和信息安全管理程序支持，包括为业务领导定义的信息安全角色和职责。
Policy Enforcement 策略实施	GRM-07	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.应建立一个正式的纪律处分或处罚政策，以应对员工违反安全策略和规程的情况。应让员工知道什么行为会引起违规事件，同时应在策略和规程中明示惩戒措施。
Policy Impact on Risk Assessments 风险评估对策略的影响	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.风险评估结果应包括更新的安全策略、规程、标准和控制措施，从而确保风险评估与它们相关并且是有效的。
Policy Reviews 策略评审	GRM-09	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.组织的业务领导（或其他负责的业务角色或部门）应按计划的时间间隔，或在组织发生变革时，评审其信息安全方针，以确保信息安全方针持续符合安全战略且有效、准确、适宜，并符合法律法规要求及合规性义务。
Risk Assessments 风险评估	GRM-10	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).应保持与企业层面的框架的一致性，至少每年或按计划的时间间隔（伴随信息系统的任何变更）开展一次正式的风险评估，使用定性和定量的方法来确定所有已识别风险的可能性和影响。固有风险和残余风险的可能性和影响应相互独立，并综合考虑所有风险类别（如：审计结果、威胁和脆弱性分析、合规性等）。

Risk Management Framework 风险管理框架	GRM-11	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.风险应控制在一个可接受的水平。应建立基于风险准则的风险接受级别并将其文件化，使其符合合理的解决时间框架并得到利益相关方的批准。
Human Resources Security 人力资源安全		
Asset Returns 资产归还	HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.当员工离职和/或外部业务关系终止时，应保证所有组织资产在规定时间内归还。
Background Screening 背景调查	HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.应根据当地的法律、法规、道德和合同约束，针对所有候选员工、承包商和第三方，根据其可访问的数据类别、业务需求和可接受风险来开展背景调查。
Employment Agreements 任用协议	HRS-03	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.就业协议应包括规定和/或既定的信息治理和安全政策，由新聘或在职员工（例如：全职、兼职或临时员工）在被授权访问企业的设施、资源和资产之前签署。
Employment Termination 任用终止	HRS-04	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.应在工作管理规程中分配执行离职或转岗的角色和职责，形成文件并传达。
Mobile Device Management 移动设备管理	HRS-05	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).应建立策略和规程，并实施支持性业务流程和技术手段，管理允许移动设备访问企业资源引起的业务风险，可能需要采用强度更高的补偿控制措施和可接受的使用策略和规程（如：强制安全培训、强化的身份标识、授权和访问控制，以及设备监控）。

Non-Disclosure Agreements 保密协议	HRS-06	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.应识别、记录反映组织数据保护和执行细节要求的不扩散或保密协议要求，并按计划的时间间隔进行评审。
Roles / Responsibilities 角色/职责	HRS-07	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.当涉及信息资产与安全时，应对承包商、员工和第三方用户的角色和责任进行文件化。
Technology Acceptable Use 技术可接受使用	HRS-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.应建立策略和规程，并实施支持性业务流程和技术手段，明确组织拥有或管理的用户终端设备（如：下发的工作站、笔记本电脑和移动设备）及 IT 基础网络和系统组件的使用条件和场合。此外，应考虑允许个人移动设备和相关的应用程序（即 BYOD）准入和访问企业资源的条件和场合。
Training / Awareness 培训/意识	HRS-09	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.应针对所有承包商、第三方用户，以及组织的员工建立安全意识培训方案，并在合适时强制执行。所有访问组织数据的人员应根据他们的专业职能，接受适当的意识培训和定期更新的组织程序和过程的培训。
User Responsibility 用户职责	HRS-10	All personnel shall be made aware of their roles and responsibilities for:所有人员应认识到他们的角色和责任： • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations.保持对既定政策、规程以及适用的法律法规和合规性义务的知晓和遵从。 • Maintaining a safe and secure working environment 维护一个安全的工作环境。

Workspace 工作场所	HRS-11	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.应建立策略和规程，要求无人值守的工作场所不存在公开可见的（如：桌面）敏感文件，要求用户计算会话在设定的不活动时间后关闭。
Identity & Access Management 身份与访问控制		
Audit Tools Access 审计工具访问	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.针对与组织的信息系统具有交互功能的审计工具，应适当隔离和限制对其的访问和使用，以防止审计日志数据被破坏和误用。
Credential Lifecycle / Provision Management 凭证生命周期/提供管理	IAM-02	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following:应建立用户访问策略和规程，并实施支持性业务流程和技术手段，确保公司内部的和客户（租户）的用户访问数据、组织所有或管理的（物理和虚拟的）的应用程序接口、基础设施网络和系统组件时，具有适当的身份、授权和访问管理。这些策略、规程、流程和措施必须包括以下内容： • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships)基于工作职能（如：内部员工和临时员工的变动、客户拜访、提供商业务关系或其他第三方业务关系），按照最小授权原则建立供给和撤销用户账号权限的程序，以及支持性角色和责任。 • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems)有关更高级保证和多因素身份验证秘密（如：管理界面、密钥生成、远程访问、职责分离、紧急通道、大规模供给或分布式部署，关键系统人员冗余）的商业论证。 • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant))在多租户架构中，对任何第三方（如：提供商、客户/租户）针对会话与数据的访问隔离。 • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation)身份可信性验证、服务到服务的 API 和信息流交互（如：SSO 和联合身份验证）。

		• Account credential lifecycle management from instantiation through revocation 账号凭证生命周期管理，从实例化到回收的全过程。 • Account credential and/or identity store minimization or re-use when feasible 如可行，账号凭证和/或身份信息存储最小化或重用。 • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets)访问数据和会话的认证、授权和记账（AAA）规则（如：加密和强/多因素认证、可过期的、非共享秘密认证信息）。 • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions 基于认证、授权和记账（AAA）规则，为客户（租户）访问数据和会话提供许可和支持能力。 • Adherence to applicable legal, statutory, or regulatory compliance requirements 遵守适用的法律法规和行业合规要求。
Diagnostic / Configuration Ports Access 诊断/配置端口访问	IAM-03	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.对诊断和配置端口的访问应仅限于授权的人员和应用程序。
Policies and Procedures 策略和规程	IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.应建立策略和规程，以存储和管理每个可访问 IT 基础设施的人员的身份信息，并确定其访问级别。同时应基于用户身份建立策略以控制对网络资源访问。
Segregation of Duties 职责分离	IAM-05	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.应建立用户访问策略和规程，并实施支持性业务流程和技术手段，按照既定的职责分离原则限制用户访问，以处理因用户角色的利益冲突而引起的业务风险。
Source Code Access Restriction 源代码访问限制	IAM-06	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.应按照既定的用户访问策略和规程，基于业务职能并遵循最小权限原则，适当限制对组织自主开发的应用、程序、目标代码或其他任何形式的知识产权（IP）的访问，以及对专有软件的使用。

Third Party Access 第三方访问	IAM-07	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.应识别、评估由于业务流程的需要，第三方访问组织信息系统和数据的风险，并排定风险的优先级。为管理这些风险，应协调应用资源，监控、测量未授权或不合适的访问的可能性和影响，并使其最小化。应在提供访问之前根据风险分析结果采取补偿措施控制风险。
Trusted Sources 可信源	IAM-08	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.针对可允许存储和访问的用于认证的身份信息，应建立策略与规程确保对身份信息的访问是基于最小权限原则，且复制仅限于明确定义为业务所需的用户。
User Access Authorization 用户访问授权	IAM-09	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.在提供用户（如：员工、承包商、客户/租户、合作伙伴和/或供应商）访问数据和组织所有或管理的（物理和虚拟的）应用程序、基础设施系统和网络组件时，用户应在被获准访问前由组织的管理层授权，并按照既定的策略和规程加以适当限制。根据要求，访问提供者应向客户（租户）通告这种用户访问情况，特别是如果客户（租户）的数据被用作服务的一部分时，和/或客户（租户）具有共同承担实施控制措施的责任时。
User Access Reviews 用户访问评审	IAM-10	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.应按计划的时间间隔，由组织的业务领导或其他负责的业务角色或职能授权和重新生效的适宜的用户访问权限，此过程需有证据证明组织遵守了基于工作职责的最小权限原则。对于违反访问控制要求的情况，须按照既定的用户访问策略和规程采取补救措施。

User Access Revocation 用户访问撤销	IAM-11	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.应按照既定的策略和规程，基于用户状态的变化（如：员工离职或其他业务关系终止、工作变动或轮换），及时撤销（取消或调整）用户访问数据、组织所有或管理的（物理和虚拟的）的应用程序、基础设施系统和网络组件的权限。根据要求，提供商应通知客户（租户）以上变化，特别是当客户（租户）的数据被用作服务的一部分时，和/或客户（租户）具有共同承担实施控制措施的责任时。
User ID Credentials 用户 ID 身份凭证	IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:为确保适当的身份标识、授权和访问管理，应依照既定的策略和规程，按以下要求限制公司内部或客户（租户）的用户账号凭证： • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation)身份标识的可信验证、服务到服务应用（API）和信息处理交互性（如：SSO 和联合身份验证）。 • Account credential lifecycle management from instantiation through revocation 从实例化到回收的账号凭证生命周期管理。 • Account credential and/or identity store minimization or re-use when feasible 如可行，账号凭据和/或身份标识存储最小化或再利用。 • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)遵守行业可接受的和/或监管合规的认证、授权、审计（AAA）规则（如：强/多因素、可过期的、非共享秘密认证信息）。
Utility Programs Access 实用程序访问	IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.应限制可能超越系统、对象、网络、虚拟机和应用程序控制措施的实用程序。

Infrastructure & Virtualization Security 基础设施与虚拟化安全		
Audit Logging / Intrusion Detection 审计日志/入侵检测	IVS-01	Higher levels of assurance are required for protection, retention, and lifecyle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.需建立对审计日志保护、保留和生命周期管理的高级别保证机制，以符合适用的法律法规和强制性义务，确保提供用户访问的唯一可追溯能力，以检测潜在的可疑网络行为和/或文件完整性异常，并提供在安全违规的情况下的取证调查能力。
Change Detection 变更检测	IVS-02	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).提供商应时刻确保所有虚拟机镜像的完整性。必须记录虚拟机镜像的任何改变并发出警报，无论其处于何种状态（如：休眠、关闭或运行中）。对于虚拟机镜像的改变、移动和随后对镜像完整性校验的结果，必须通过电子方式（如：门户网站或告警信息）让客户能够立即获取到。
Clock Synchronization 时钟同步	IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.应使用一个可靠且经双向认可的外部时钟源，对所有相关信息处理系统的系统时钟进行同步，以便跟踪和重建活动时间表。
Information System Documentation 信息系统记录	IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.应对可用性、质量以及适度的容量和资源进行计划、准备和测量，以符合法律法规和强制性义务要求的系统性能。应预测未来的容量需求以减少系统过载的风险。
Vulnerability Management 脆弱性管理	IVS-05	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g.virtualization aware).执行者应确保安全漏洞评估工具或服务适应当前使用的虚拟化技术（如虚拟化感知）。

Network Security 网络安全	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.应设计并配置网络环境和虚拟机实例，以限制和监控可信与不可信通信中的流量。应至少每年对这些配置进行一次评审，书面说明所有允许的服务、协议和端口的使用理由，并建立补偿性控制措施。
OS Hardening and Base Conrols 操作系统加固和基础控制措施	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.应对每个操作系统进行加固，以提供业务必需的端口、协议和服务，并落实技术控制措施，如：杀毒软件、文件完整性监控、日志记录等，这些可以作为其运行构建的基线标准或模板的一部分。
Production / Non-Production Environments 生产/非生产环境	IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.应隔离生产和非生产环境，以防止对信息资产的未授权访问或变更。环境隔离的手段可包括：状态检测防火墙、域认证源、人员因本职工作需访问该环境时的明确的职责分离。
Segmentation 隔离	IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:应设计、开发、部署、配置多租户情况下组织所有或管理的（物理和虚拟的）应用程序、基础设施系统和网络组件，在提供商和客户（租户）之间，以及租户之间提供用户访问隔离，在隔离时基于以下考虑： • Established policies and procedures 既定的策略和规程。 • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance 隔离关键业务资产和/或敏感用户数据及会话时，使用更强的内部控制措施和更高级别的保证。 • Compliance with legal, statutory and regulatory compliance obligations 符合法律法规和强制性义务的要求。

VM Security - vMotion Data Protection 虚拟机安全-迁移数据保护	IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations. 当将物理服务器、应用程序或数据向虚拟服务器迁移时，应使用安全、加密的信道，如可能，还应使用一个与生产级别网络隔离的网络完成迁移。
VMM Security - Hypervisor Hardening 虚拟机监控器安全-加固	IVS-11	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).当访问虚拟机监控器的管理功能或宿主系统的管理控制台时，应基于最小权限原则限制人员访问，并采用技术控制措施（如：双因素认证、审计追踪、IP 地址过滤、防火墙、TLS 协议和管理控制台通信）。
Wireless Security 无线安全	IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following:应建立策略和规程，并实施支持性业务流程和技术手段，保护无线网络环境，包括以下内容： • Perimeter firewalls implemented and configured to restrict unauthorized traffic 部署和配置边界防火墙以限制非授权流程。 • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)对认证和传输启用强加密的安全设置，以替代厂商的默认设置（如：加密密钥、口令和 SNMP 社区字符串）。 • User access to wireless network devices restricted to authorized personnel 仅允许授权人员访问无线网络设备。 • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network 检测未授权的（流氓）无线网络设备并及时断开与其网络连接的能力。
Network Architecture 网络架构	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.网络架构图应清楚地识别可能有法律合规性影响的高风险环境和数据流。应实施技术措施和深度防御技术（如：深度包分析、流量抑制和黑洞）检测并及时响应和出入站异常流量模式相关的基于网络的攻击（如：MAC 欺骗和 ARP 中毒攻击）和/或分布式拒绝服务（DDoS）攻击。

Interoperability & Portability 互操作与可移植性

APIs 应用程序接口	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.提供商应使用开放和已发布的 API 来为组件之间的互操作提供支持，以及实现对应用的迁移。
Data Request 数据请求	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)应将所有结构化和非结构化的数据以行业标准格式向客户提供（如：DOC、XLS、PDF、日志和纯文本文件）。
Policy & Legal 策略和法规	IPY-03	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.建立策略、规程和以及双方同意基础上的规定和/或条款，以满足客户（租户）服务到服务应用（API）和信息处理互操作性的要求、应用程序开发和信息交换使用的可移植性、完整性保持的要求。
Standardized Network Protocols 标准化网络协议	IPY-04	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.提供商应使用安全的（如：非明文且经过认证的）标准网络协议，以输入和输出数据并管理服务，还应向客户（租户）提供详细介绍相关互操作性和可移植性标准的文件。
Virtualization 虚拟化	IPY-05	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.提供商应使用行业公认的虚拟化平台和标准虚拟化格式（如：OVF）来确保互操作性，针对使用中的虚拟机监控器以及特定解决方案的虚拟化钩子程序的任何自定义变更都应记录并在用户审查时保持可用。

Mobile Security 移动安全

Anti-Malware 防护恶意软件	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.应将针对移动设备的防恶意程序意识培训纳入提供商信息安全意识培训之中。
Application Stores 应用程序商店	MOS-02	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.针对能访问和存储提供商管理数据的移动设备，定义一个可接受的且通过审批的应用商店的文档化列表。
Approved Applications 授权的应用程序	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.公司应建立一个文件化策略禁止安装那些未经批准或已批准但不是通过已鉴定的应用商店获取的应用程序。
Approved Software for BYOD BYOD 的授权软件	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.通过 BYOD 策略和相关意识培训明确规定可供 BYOD 使用的经批准的应用程序、应用程序商店以及应用扩展插件。
Awareness and Training 意识和培训	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.提供商应建立一个文件化的移动设备策略，包括对移动设备的文件化定义和所有移动设备的使用条件和要求。提供商应通过公司安全意识宣导和培训方案发布和传达该策略。
Cloud Based Services 基于云的服务	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.所有用于访问云服务的公司移动设备或 BYOD，应提前得到批准方可使用和存储公司业务数据。

Compatibility 兼容性	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.公司应建立文件化的应用程序验证流程，用于测试移动设备、操作系统和应用程序的兼容性问题。
Device Eligibility 设备资格	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.BYOD 策略应规定允许使用的 BYOD 设备和使用 BOYD 的资格要求。
Device Inventory 设备目录	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.应保存并维护一份可以存储和访问公司数据的移动设备清单。清单中应包括每台设备的所有状态变化（如：操作系统和补丁级别、丢失或退役的状态、（BYOD）被分配或授权的使用人）。
Device Management 设备管理	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.应针对可以存储、传输或处理客户数据的移动设备，建立一个集中化的移动设备管理解决方案。
Encryption 加密	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.移动设备策略应要求对整个设备和其中的敏感数据进行加密，并通过技术控制措施实现。
Jailbreaking and Rooting 越狱和获得最高权限	MOS-12	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).移动设备策略应禁止出现破坏移动设备内置安全控制措施的行为（如：越狱或获得最高权限），并通过集中式移动设备管理系统的检测和预防性控制功能来强化禁令的执行。

Legal 法规	MOS-13	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case a wipe of the device is required. BYOD策略中应明确注明个人隐私、诉讼需求、电子发现、法律证据方面的内容。BYOD策略应明确声明非公司的数据会在对设备进行数据擦除时随之丢失。
Lockout Screen 锁屏	MOS-14	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.应要求通过技术手段将BYOD和/或公司设备配置成自动锁屏。
Operating Systems 操作系统	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.应通过公司的变更管理流程管理移动设备操作系统、补丁级别和应用程序的变更。
Passwords 口令	MOS-16	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.应文件化并通过技术手段实现公司设备或授权使用的BYOD的移动设备口令策略，并禁止对口令/PIN长度和认证要求的变更。
Policy 策略	MOS-17	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).移动设备策略应要求BYOD用户执行数据备份，禁止使用非授权应用商店，以及（在设备支持的情况下）使用防恶意程序软件。
Remote Wipe 远程擦除	MOS-18	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.公司BYOD方案允许使用的所有移动设备或是公司配发的移动设备，应允许公司的企业IT远程擦除设备或公司提供的数据。

Security Patches 安全补丁	MOS-19	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.对于可连接到企业网络，或存储和访问公司信息的移动设备，应允许对其进行远程软件版本/补丁验证。应保证所有移动设备能获取由设备制造商或运营商发布的最新的安全补丁，同时允许授权的 IT 人员执行更新远程。
Users 用户	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.BYOD 策略应明确在 BYOD 设备上可以访问和使用的系统和服务器。
Security Incident Management, E-Discovery & Cloud Forensics **安全事件管理，电子发现与云取证**		
Contact / Authority Maintenance 联络人/监管机构维护	SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.和相关监管机构、国家和地方执法机关以及其他法律管辖机关之间联络点应加以维护和定期更新（如：在影响范围和/或任何合规义务发生变化时），确保已建立直接联系，并为各类取证调查能迅速加入执法过程做好准备。
Incident Management 事件管理	SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.应建立用户访问策略和规程，并实施支持性业务流程和技术手段，以分类安全相关事态，并确保符合既定 IT 服务管理策略和规程的及时且全面的事件管理。
Incident Reporting 事件报告	SEF-03	Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.应向员工和外部业务关系告知他们的责任，必要时，应采用双方认可的形式和/或通过合同形式要求他们及时报告所有信息安全事件。应通过预定义的沟通渠道及时报告地信息安全事态，并遵守适用的法律法规或强制性义务。

Incident Response Legal Preparation 事件响应法律准备	SEF-04	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.在发生信息安全事件后，根据相关司法管辖区要求，需要适当的司法程序（包括监管链），提供证据来支持潜在的法律行动。在接到通知后，应给予受安全违规影响的客户和/或其他外部业务伙伴基于法律许可参与调查取证的机会。
Incident Response Metrics 事件响应度量指标	SEF-05	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.应落实监测、量化信息安全事件类型、数量和成本的机制。
Supply Chain Management, Transparency and Accountability 供应链管理，透明与可审计		
Data Quality and Integrity 数据质量和完整性	STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.提供商应检查、负责并与他们的云供应链合作伙伴一起纠正数据质量错误及相关风险。提供商应对其供应链内的所有人员采用适当的职责分离、基于角色的访问、最小权限原则，设计并实施控制措施以缓解和遏制数据安全风险。
Incident Reporting 事件报告	STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g. portals).提供商应定期通过电子方式（如：门户网站）将安全事件的信息提供给所有受影响的客户和提供商。
Network / Infrastructure Services 网络/基础设施服务	STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.针对关键业务或受影响客户（租户）的（物理和虚拟的）应用系统接口（API）的设计和配置，以及基础网络和系统组件，应按照双方商定的服务水平和能力期望，以及 IT 治理和服务管理策略和规程进行设计、开发和部署。
Provider Internal Assessments 供应商内部评估	STA-04	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.提供商应每年对策略、规程及配套措施和指标的符合性和有效性进行内部评估。

Supply Chain Agreements 供应链协议	STA-05	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms:提供商和客户（租户）之间的供应链协议（如：SLA）应至少包括以下双方同意的规定和/或条款： • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations)业务关系和服务提供（如：客户（租户）数据获取、交换和使用；特征集和功能点；用于服务交付和支持的人员、基础网络和系统组件；云服务提供商、客户（租户）、分包商或外包业务的角色和责任；托管服务的地理位置；以及任何已知的监管合规考虑）的范围。 • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships 信息安全要求；提供商与租户(客户)在业务存续期间的主要联络点；精细化支撑相关参考；针对所有受影响的业务关系实施有效的治理、风险管理、保证、法律法规及监管合规义务的相关业务流程与技术措施。 • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts 任何由提供商控制并对客户（租户）产生影响的变更的通知和/或预授权。 • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain)及时向所有客户（租户）和其它业务关系（即受影响的供应链上、下游）通知产生影响的安全事件（或已确认的破坏）。 • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed 不造成产生被评估组织不可接受风险的，符合协议规定和/或条款（例如：行业认可的认证、审核报告或同等形式的保证）的评估和独立验证。 • Expiration of the business relationship and treatment of customer (tenant) data impacted 业务关系到期以及对受影响的客户（租户）数据的处置。 • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence 用于应用程序开发和信息交换、使用及保持完整性的客户（租户）服务到服务的应用程序（API）和数据互操作性和可移植性的要求。

Supply Chain Governance Reviews 供应链治理评审	STA-06	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.提供商应评审其合作伙伴的风险管理和治理流程，以确保合作伙伴对从其供应链其他成员那里继承的风险负责。
Supply Chain Metrics 供应链度量	STA-07	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream).应实施策略和规程，以确保能够对提供商和客户（租户）跨越相关供应链（上下游）的服务协议（如：SLAs）的持续评审。 Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.评审应至少每年进行一次，并根据已签订协议识别不符合。评审结果应触发行动去处理由不同供应商引起的服务级别冲突或不一致。
Third Party Assessment 第三方评估	STA-08	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.提供商应通过年度评审保证跨信息供应链的合理的信息安全。评审应包括信息供应链所依赖的所有合作伙伴/第三方提供商。
Third Party Audits 第三方审核	STA-09	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.第三方服务提供商应证明其符合信息安全、保密、访问控制、服务定义以及包括在第三方合同中的交付级别协议的要求。为管控和维护服务交付协议，第三方报告、记录和服务应至少每年接受审核和评审。

Threat and Vulnerability Management 威胁、脆弱性管理		
Anti-Virus / Malicious Software 防病毒/恶意软件	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.应建立策略和规程，并实施支持性业务流程和技术手段，以防止恶意软件在组织所有或管理的用户终端设备（即：工作站、笔记本电脑和移动设备）以及 IT 基础设施网络和系统组件上执行。
Vulnerability / Patch Management脆弱性/补丁管理	TVM-02	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identfied weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.应建立策略和规程，并实施支持性业务流程和技术手段（如：网络脆弱性评估、渗透测试），及时检测在组织所有或管理的应用程序、基础网络和系统组件中的脆弱性，以确保实施安全控制措施的有效性。应使用一个基于风险的模型优先修复已发现的漏洞。应通过变更管理流程管理变更，如：厂商提供的补丁、配置变更或组织自主开发的软件的变更。根据要求，提供商应向客户（租户）告知策略、规程和已识别的弱点，特别是当客户（租户）的数据被用作服务的一部分和/或客户（租户）具有共同承担实施控制措施的责任时。
Mobile Code 移动代码	TVM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.应建立策略和规程，并实施支持性业务流程和技术手段，以防止非授权的移动代码在组织所有或管理的用户终端设备（如：工作站、笔记本电脑和移动设备）以及 IT 基础设施网络和系统组件上执行。移动代码的定义为在可信或不可信网络中的系统之间传输、在本地系统执行且无需接受者主动安装或执行的软件。