Alibaba Cloud

Alibaba Cloud Responses to CSA CAIQ v3.0.1

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
Application and Interface Security: Controls AIS-01 through AIS-04						
AIS-01.1: Application & Interface Security - Application Security	*Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?*	Y			是，阿里云已参考ISO27001等国际标准及相应最佳实践建立了云产品安全生命周期（Secure Product Lifecycle，简称SPLC），是阿里云为云上产品量身定制的云产品安全生命周期，目标是将安全融入到整个产品开发生命周期中。	Yes, Alibaba Cloud has established a Cloud Secure Product Lifecycle (SPLC) with reference to international standards such as ISO27001 and corresponding best practices. Integrate security into the entire product development life cycle.
AIS-01.2: Application & Interface Security - Application Security	*Do you use an automated source code analysis tool to detect security defects in code prior to production?*	Y			是，阿里云遵循SPLC流程中的规定，通过自动化的代码安全扫描工具进行代码库的扫描，保证代码扫描未通过的产品、未通过人工代码安全审核的产品均无法正式上线。详细的控制措施见SOC2/3报告。	Yes, Alibaba Cloud follows the rules in the SPLC process and scans the code base through an automated code security scanning tool to ensure that products that fail the code scan and products that fail the manual code security audit cannot be officially launched. Detailed control measures can be found in the SOC2/3 report.
AIS-01.3: Application & Interface Security - Application Security	*Do you use manual source-code analysis to detect security defects in code prior to production?*	Y			是，阿里云遵循SPLC流程中的规定，通过自动化的代码安全扫描工具进行代码库的扫描，保证代码扫描未通过的产品、未通过人工代码安全审核的产品均无法正式上线。详细的控制措施见SOC2/3报告。	Yes, Alibaba Cloud follows the rules in the SPLC process and scans the code base through an automated code security scanning tool to ensure that products that fail the code scan and products that fail the manual code security audit cannot be officially launched. Detailed control measures can be found in the SOC2/3 report.
AIS-01.4: Application & Interface Security - Application Security	*Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?*	Y			是，阿里云已有制定供应商管理规范，且在针对供应商的安全管理要求中明确了其信息安全管理体系的符合性，同时针对所有上线的云产品均应通过架构评审、安全技术评审和合规评审，以保证对于涉及第三方软件供应商的场景可以满足阿里云的安全要求后方可产品上线。	Yes, Alibaba Cloud has established supplier management policy, and has clarified the compliance of its information security management system in the security management requirements for suppliers. At the same time, all cloud products that have gone online should pass architecture review, security technology review, compliance review to ensure that the scenarios involving third-party software vendors can meet the security requirements of Alibaba Cloud before the product goes online.
AIS-01.5: Application & Interface Security - Application Security	*(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?*	Y			是，阿里云遵循SPLC流程中的规定，通过自动化的代码安全扫描工具进行代码库的扫描，保证代码扫描未通过的产品、未通过人工代码安全审核的产品均无法正式上线。详细的控制措施见SOC2/3报告。	Yes, Alibaba Cloud follows the rules in the SPLC process and scans the code base through an automated code security scanning tool to ensure that products that fail the code scan and products that fail the manual code security audit cannot be officially launched. Detailed control measures can be found in the SOC2/3 report.
AIS-02.1: Application & Interface Security - Customer Access Requirements	*Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?*	Y			是，阿里云通过面向客户的法律各类协议、权威第三方审计/认证和云安全白皮书等多种形式来说明云平台自身的安全能力。	Yes, Alibaba Cloud demonstrates the security capabilities of the cloud platform through various forms of customer-oriented legal agreements, authoritative third-party audits/certifications, and cloud security white papers.
AIS-02.2: Application & Interface Security - Customer Access Requirements	*Are all requirements and trust levels for customers' access defined and documented?*	Y			是，基于共担责任模型，由阿里云保障云平台自身安全并提供安全产品和能力给云上客户，且由客户负责基于阿里云服务构建的应用系统的安全。	Yes, the security of applications built on Alibaba Cloud is the joint responsibility of Alibaba Cloud and the customers. Alibaba Cloud is responsible for the security of the underlying cloud service platform and providing security services and capabilities to customers, while customers are responsible for the security of applications built based on Alibaba Cloud services.
AIS-03.1: Application & Interface Security - Data Integrity	*Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?*	Y			是，阿里云基于数据安全管理策略，通过访问控制实现只有合法的（或预期的）用户才能修改数据，同时在数据的传输和存储中可以通过校验算法来加强用户数据的完整性保护。	Yes, based on data security management policies, only legitimate (or expected) users can modify data through access control. At the same time, the integrity protection of user data can be enhanced by verifying algorithms in data transmission and storage.
AIS-04.1: Application & Interface Security - Data Security/Integrity	*Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?*	Y			是，阿里云基于自身业务运营的需求涉及了数据安全架构，并通过第三方权威认证来证明数据安全架构的符合性，如ISO 27001、SOC 2/3报告等。	Yes, the requirements of Alibaba Cloud based on its own business operations involve data security architecture, and certification of data security architecture is verified by third-party authority certifications, such as ISO 27001, SOC 2/3 reports, etc.
Audit Assurance and Compliance: Controls AAC-01 through AAC-03						
AAC-01.1: Audit Assurance & Compliance - Audit Planning	*Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?*	Y			是，阿里云先后通过了海内外数十家第三方权威机构的认证和审计，如ISO 27001、SOC2/3报告。	Yes, Alibaba Cloud has passed certifications and audits of dozens of third-party authorities globally, such as ISO 27001 and SOC2/3 reports.
AAC-02.1: Audit Assurance & Compliance - Independent Audits	*Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?*	Y			是，阿里云设立了相关渠道将SOC2/3报告、ISO27001认证的证书提供给客户，国内业务的证书可通过阿里云的工单系统申请，国际业务的证书可通过官网信任中心获取。	Yes, Alibaba Cloud has established relevant channels to provide customers with SOC2/3 reports and ISO27001 certificate. Certificates for domestic business can be applied through Alibaba Cloud's ticketing system, and certificates for international business can be obtained through the official website trust center.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
AAC-02.2: Audit Assurance & Compliance - Independent Audits	*Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?*	Y			是，阿里云建立云平台侧红蓝对抗计划，通过组织具备黑客能力的专家成立蓝军队伍，充分施展黑客攻击技术和渗透思路（不限时间、不限技术、不限范围），以周期实战性质的攻防对抗方式找出云平台最脆弱的环节，客观检验阿里云安全防御能力、威胁检测能力的水位，提升阿里云核心安全能力，完善平台防御体系。	Yes, Alibaba Cloud establishes a red and blue team confrontation plan on the side of the cloud platform. By organizing experts with hacking capabilities to set up a blue team, it fully implements hacking techniques and penetration ideas (unlimited time, unlimited technology, and unlimited scope). The offensive and defensive methods of nature find out the most vulnerable part of the cloud platform, objectively test the level of Alibaba Cloud's security defense capabilities and threat detection capabilities, improve Alibaba Cloud's core security capabilities, and improve the platform's defense system.
AAC-02.3: Audit Assurance & Compliance - Independent Audits	*Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance?*	Y			是，阿里云建立云平台侧红蓝对抗计划，通过组织具备黑客能力的专家成立蓝军队伍，充分施展黑客攻击技术和渗透思路（不限时间、不限技术、不限范围），以周期实战性质的攻防对抗方式找出云平台最脆弱的环节，客观检验阿里云安全防御能力、威胁检测能力的水位，提升阿里云核心安全能力，完善平台防御体系。	Yes, Alibaba Cloud establishes a red and blue team confrontation plan on the side of the cloud platform. By organizing experts with hacking capabilities to set up a blue team, it fully implements hacking techniques and penetration ideas (unlimited time, unlimited technology, and unlimited scope). The offensive and defensive methods of nature find out the most vulnerable part of the cloud platform, objectively test the level of Alibaba Cloud's security defense capabilities and threat detection capabilities, improve Alibaba Cloud's core security capabilities, and improve the platform's defense system.
AAC-02.4: Audit Assurance & Compliance - Independent Audits	*Do you conduct internal audits regularly as prescribed by industry best practices and guidance?*	Y			是，阿里云基于合规需求和行业最佳实践执行定期的内部审计。	Yes, Alibaba Cloud performs regular internal audits based on compliance requirements and industry best practices.
AAC-02.5: Audit Assurance & Compliance - Independent Audits	*Do you conduct external audits regularly as prescribed by industry best practices and guidance?*	Y			是，阿里云基于第三方权威认证及审计的需求执行定期的外部审计，如SOC 1/2/3、ISO 27001系列等。	Yes, Alibaba Cloud performs regular external audits based on the requirements of third-party authority certification and auditing, such as SOC 1/2/3, ISO 27001 series, etc.
AAC-02.6: Audit Assurance & Compliance - Independent Audits	*Are the results of the penetration tests available to tenants at their request?*		N		否，阿里云云平台侧的渗透测试结果由云平台自行跟进。	No, the penetration test results on the side of Alibaba Cloud platform will be followed up by the cloud platform itself.
AAC-02.7: Audit Assurance & Compliance - Independent Audits	*Are the results of internal and external audits available to tenants at their request?*	Y			是，阿里云定期开展内部审计和第三方权威审计，一旦客户对阿里云的审计结果有需求，阿里云会基于客户的需求和阿里云的数据安全管理要求将审计结果提供给客户。	Yes, Alibaba Cloud regularly conducts internal audits and third-party audits. Once customers have requirements for Alibaba Cloud's audit results, Alibaba Cloud can share audit results to customers based on their needs as well as Alibaba Cloud's data security management requirements.
AAC-02.8: Audit Assurance & Compliance - Independent Audits	*Do you have an internal audit program that allows for cross-functional audit of assessments?*	Y			是，阿里云引入了各职能方参与内部审计工作，以保证内部审计团队能够覆盖到阿里云各领域。	Yes, Alibaba Cloud has introduced various functional parties to participate in internal audit work to ensure that the internal audit team can cover all areas of Alibaba Cloud.
AAC-03.1: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?*	Y			是，阿里云通过虚拟化技术，包括CPU隔离、内存隔离、存储隔离和网络隔离实现租户间的资源隔离。同时，阿里云提供存储加密的产品能力供用户根据需求执行数据加密，如EBS、OSS、RDS、Table store、NAS、Maxcompute等产品均支持存储加密功能，用户可使用阿里云的KMS产品进行密钥管理。	Yes, Alibaba Cloud implements resource isolation between tenants through virtualization technologies including CPU isolation, memory isolation, storage isolation, and network isolation. At the same time, Alibaba Cloud provides storage encryption product capabilities for users to perform data encryption according to their needs. For example, EBS, OSS, RDS, Table Store, NAS, Maxcompute and other products support storage encryption. Users can use Alibaba Cloud's KMS product for keys management.
AAC-03.2: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have capability to recover data for a specific customer in the case of a failure or data loss?*	Y			是，阿里云在产品文档内与客户说明可提供数据恢复能力的方式与限制。	Yes, Alibaba Cloud explains to customers in the product documentation the ways and limitations to provide data recovery capabilities.
AAC-03.3: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?*	Y			是，用户在购买产品时可选择数据存储的可用区。	Yes, the user can select the Availability Zone of the data store when purchasing the product.
AAC-03.4: Audit Assurance & Compliance - Information System Regulatory Mapping	*Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?*	Y			是，阿里云会持续监控业务符合性以保证满足变化的外部监管合规环境。阿里云的用户需要基于其业务所应满足的监管合规要求，保证对其应满足的监管合规要求的符合度。	Yes, Alibaba Cloud will continuously monitor business compliance to ensure that the changing external regulatory compliance environment is met. Alibaba Cloud users need to ensure compliance with the regulatory compliance requirements they should meet based on the regulatory compliance requirements according to their business needs.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
Business Continuity Management and Operational Resilience: Controls BCR- 01 through BCR-11						
BCR-01.1: Business Continuity Management & Operational Resilience - Business Continuity Planning	*Do you provide tenants with geographically resilient hosting options?*	Y			是，阿里云在全球提供多可用区给客户选择，且客户可依照自身需求挑选特定可用区。最新的可用区开服状况，请参考阿里云官网：https://www.alibabacloud.com/global-locations。	Yes, Alibaba Cloud provides multiple Availability Zones for customers to choose from, and customers can choose specific Availability Zones according to their needs. For the latest availability zone availability status, please refer to Alibaba Cloud's official website: https://www.alibabacloud.com/global-locations.
BCR-01.2: Business Continuity Management & Operational Resilience - Business Continuity Planning	*Do you provide tenants with infrastructure service failover capability to other providers?*		N		否，但客户可依照自身需求，选择多可用区实现冗余机制。	No, but customers can choose Multi-AZ to implement redundancy mechanism according to their own needs.
BCR-02.1: Business Continuity Management & Operational Resilience - Business Continuity Testing	*Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?*	Y			是，阿里云已参考ISO27001及ISO22301等国际标准及相应最佳实践，建立业务连续性计划并定期测试	Yes, Alibaba Cloud has referenced international standards such as ISO27001 and ISO22301 and corresponding best practices to establish business continuity plans and regularly test
BCR-03.1: Datacenter Utilities/Environmental Conditions	*Do you provide tenants with documentation showing the transport route of their data between your systems?*		N		否，客户可以自行选择一个区域或数据中心存储其数据内容。无论客户将其数据内容存储在哪个区域或数据中心，客户都可以对其进行有效的控制，在没有客户授权的情况下，这些数据不会离开客户选择的区域或数据中心。阿里云所有的数据中心皆有维护相应的网络拓朴图，但因该信息属于内部敏感信息，故不对客户公开。然而，客户可在签署NDA的状况，向阿里云获取SOC2/3报告，理解网络管理的相应控制概要。	No, the customer can choose a region or data center to store its data. No matter which region or data center the customer stores its data content, the customer can effectively control it. Without the customer's authorization, these data does not leave the customer's chosen region or data center.\n\nAll Alibaba Cloud data centers maintain corresponding network topologies, due to sensitivity, it is not disclosed to customers. However, customers can obtain the SOC2 / 3 report from Alibaba Cloud when the NDA is signed, and understand the corresponding control summary of network management.
BCR-03.2: Business Continuity Management & Operational Resilience - Datacenter Utilities/Environmental Conditions	*Can tenants define how their data is transported and through which legal jurisdictions?*		N		否，客户可依照自身需求，挑选期望数据存储的可用区，但无法选择数据流动的路径	No, customers can choose the availability zone where data is expected to be stored according to their own needs, but cannot choose the path of data flow
BCR-04.1: Business Continuity Management & Operational Resilience - Documentation	*Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?*	Y			是，阿里云依循相关国际标准建立信息系统相关文档，授权员工皆可访问相应的文档信息	Yes, Alibaba Cloud establishes information system related documents in accordance with relevant international standards, and authorized employees can access the corresponding document information
BCR-05.1: Business Continuity Management & Operational Resilience - Environmental Risks	*Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?*	Y			是，数据中心周边皆有建立相应的物理保护机制，且该机制定期由三方审计进行查核	Yes, corresponding physical protection mechanisms are established around the data center, and this mechanism is regularly checked by a third-party audit
BCR-06.1: Business Continuity Management & Operational Resilience - Equipment Location	*Are any of your data centers located in places that have a high probability/occurre nce of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?*		N		否，阿里云于数据中心选址阶段，接会对高危环境进行评估，确保数据中心避免建置于高危环境	No, during the data center site selection phase, Alibaba Cloud will assess the high-risk environment to ensure that the data center is not built in a high-risk environment
BCR-07.1: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?*	Y			是，数据中心内的硬盘皆支持热拔插机制	Yes, all hard drives in the data center support hot-plugging mechanism
BCR-07.2: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?*	Y			是，阿里云弹性计算服务提供客户快照与镜像能力，客户可导出或导入镜像，具体信息请参考官网产品文档	Yes, Alibaba Cloud Elastic Computing Service provides customers with snapshot and mirroring capabilities. Customers can export or import images. For details, please refer to the official website product documentation.
BCR-07.3: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?*	Y			是，阿里云弹性计算服务提供客户快照与镜像能力，客户可导出或导入镜像，具体信息请参考官网产品文档	Yes, Alibaba Cloud Elastic Computing Service provides customers with snapshot and mirroring capabilities. Customers can export or import images. For details, please refer to the official website product documentation.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
BCR-07.4: Business Continuity Management & Operational Resilience - Equipment Maintenance	*If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?*	Y			是，阿里云弹性计算服务提供客户快照与镜像能力，客户可导出或导入镜像，具体信息请参考官网产品文档	Yes, Alibaba Cloud Elastic Computing Service provides customers with snapshot and mirroring capabilities. Customers can export or import images. For details, please refer to the official website product documentation.
BCR-07.5: Business Continuity Management & Operational Resilience - Equipment Maintenance	*Does your cloud solution include software/provider independent restore and recovery capabilities?*	Y			是，阿里云提供了迁云工具，通过快照（EBS Snapshot）来人工或者定期Backup，详见阿里云安全白皮书。	Yes, Alibaba Cloud provides cloud migration tools, which can be manually or regularly backed up via EBS Snapshot. For details, see the Alibaba Cloud Security White Paper.
BCR-08.1: Business Continuity Management & Operational Resilience - Equipment Power Failures	*Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?*	Y			是，阿里云数据中心内已有配置冗余与相应保安机制，降低服务故障可能造成的影响，相关的信息可在阿里云SOC 2/3审计报告内查看。	Yes, the Alibaba Cloud data center has been configured with redundancy and corresponding security mechanisms to reduce the possible impact of service failures. Related information can be viewed in the Alibaba Cloud SOC 2/3 audit report.
BCR-09.1: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?*	Y			是，阿里云提供了云监控产品，让客户可以通过可视化的方式查看资源运行状况	Yes, Alibaba Cloud provides cloud monitoring products, allowing customers to visually check the resource operation status
BCR-09.2: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?*	Y			是，云监控产品让用户可以在仪表板上查看相应监控数据，并且可于信任中心下载相应的合规资质	Yes, cloud monitoring products allow users to view the corresponding monitoring data on the dashboard and download the corresponding compliance qualifications in the trust center
BCR-09.3: Business Continuity Management & Operational Resilience - Impact Analysis	*Do you provide customers with ongoing visibility and reporting of your SLA performance?*	Y			是，阿里云提供了云监控产品，让客户可以通过可视化的方式查看资源运行状况	Yes, Alibaba Cloud provides cloud monitoring products, allowing customers to visually check the resource operation status
BCR-10.1: Business Continuity Management & Operational Resilience - Policy	*Are policies and procedures established and made available for all personnel to adequately support services operations' roles?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立相关日常运维文档，阿里云所有员工皆可依照职责访问相应的文档信息	Yes, Alibaba Cloud establishes relevant daily operation and maintenance documents in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.). All Alibaba Cloud employees can access the corresponding document information according to their responsibilities.
BCR-11.1: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have technical control capabilities to enforce tenant data retention policies?*	Y			是，阿里云在服务协议内描述了数据保留期限的规则。此外，阿里云产品提供客户存储与删除数据的能力，但数据的控制与管理权由客户负责，存储规则亦由客户依照自身需求配置	Yes, Alibaba Cloud describes the rules for data retention periods in the service agreement. In addition, Alibaba Cloud products provide customers with the ability to store and delete data, but the control and management of data is the responsibility of the customer, and storage rules are also configured by the customer according to their own needs
BCR-11.2: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have a documented procedure for responding to requests for tenant data from governments or third parties?*	Y			是，客户一般可通过阿里云的工单系统提出对阿里云相关的资质、说明报告等信息，一旦属于客户合理的要求，阿里云均会及时响应客户的需求。同时，阿里云也在探索更多增加透明度的方式，通过将与特定客户相关的内部操作透传给客户的方式，进一步消除客户对阿里云内部"黑盒"的疑虑。这种突破了静态展示的界限而主动将动态的信息传递给客户的方式，将是阿里云"透明度"的长期方向。	Yes, customers can submit tickets to request information such as Alibaba Cloud qualifications and explanatory reports through the Alibaba Cloud ticket system. Alibaba Cloud will respond to any reasonable requests of customers in a timely manner. Alibaba Cloud is also exploring ways to increase transparency, such as by disclosing relevant internal operations to customers. In turn, Alibaba Cloud wishes to eliminate customers' doubts about any "black box operations" from a cloud provider. Such an approach will be the long-term direction and continuous effort of Alibaba Cloud towards transparency.
BCR-11.3: Business Continuity Management & Operational Resilience - Retention Policy	*Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?*	Y			是，阿里云负责基础设施的冗余与备份机制，并且定期进行测试与校验。且定期的三方审计也会针对机制内容进行审计确认	Yes, Alibaba Cloud is responsible for infrastructure redundancy and backup mechanisms, and conducts regular testing and verification. And regular third-party audits will also audit and confirm the content of the mechanism
BCR-11.4: Business Continuity Management & Operational Resilience - Retention Policy	*Do you test your backup or redundancy mechanisms at least annually?*	Y			是，阿里云依循相关国际标准（如ISO27001/22301）建立冗余与备份机制，且至少每年进行一次测试	Yes, Alibaba Cloud establishes redundancy and backup mechanisms in accordance with relevant international standards (such as ISO27001/22301) and tests at least once a year
BCR-11.5: Business Continuity Management & Operational Resilience - Retention Policy	*Do you have technical control capabilities to enforce tenant data retention policies?*	Y			是，阿里云会定期进行冗余与备份机制的测试。同时，客户需要依照业务场景目的在云产品上配置相应的数据存储时间	Yes, Alibaba Cloud regularly tests the redundancy and backup mechanisms. At the same time, the customer needs to configure the corresponding data storage time on the cloud product according to the purpose of the business scenario
Change Control & Configuration Management: Controls CCC-01 through CCC-05						
CCC-01.1: Change Control & Configuration Management - New	*Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立相关文档体系，且客户可在阿里云官网查看产品相关的操作手册信息	Yes, Alibaba Cloud establishes related management systems in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.), and customers can view product-related operation manual information on the Alibaba Cloud official website

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
CCC-01.2: Change Control & Configuration Management - New	*Is documentation available that describes the installation, configuration and use of products/services/features?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立相关文档体系，且客户可在阿里云官网查看产品相关的操作手册信息	Yes, Alibaba Cloud establishes related management systems in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.), and customers can view product-related operation manual information on the Alibaba Cloud official website
CCC-02.1: Change Control & Configuration Management - Outsourced Development	*Do you have controls in place to ensure that standards of quality are being met for all software development?*	Y			是，虽阿里云并没有委外开发的产品或软件，但阿里云仍依循相关国际标准建立校验流程。	Yes, although Alibaba Cloud does not have outsourced products or software, Alibaba Cloud has establishes a verification process in accordance with relevant international standards.
CCC-02.2: Change Control & Configuration Management - Outsourced Development	*Do you have controls in place to detect source code security defects for any outsourced software development activities?*	Y			是，虽阿里云并没有委外开发的产品或软件，但阿里云仍依循相关国际标准建立校验流程	Yes, Alibaba Cloud establishes related management systems in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.), and customers can view product-related operation manual information on the Alibaba Cloud official website
CCC-03.1: Change Control & Configuration Management - Quality Testing	*Do you provide your tenants with documentation that describes your quality assurance process?*	Y			是，阿里云已通过ISO9001的认证，并且由三方审计确认阿里云确实建立质量管理体系相关文档	Yes, Alibaba Cloud has passed ISO9001 certification, and a third-party audit confirmed that Alibaba Cloud has indeed established quality management system related documents
CCC-03.2: Change Control & Configuration Management - Quality Testing	*Is documentation describing known issues with certain products/services available?*	Y			是，阿里云已通过ISO9001的认证，并且由三方审计确认阿里云确实建立质量管理体系相关文档。此外，阿里云官网的文档页面也对外提供了产品/服务相应文档	Yes, Alibaba Cloud has passed ISO9001 certification, and a third-party audit confirmed that Alibaba Cloud has indeed established quality management system related documents

Yes, Alibaba Cloud has passed ISO9001 certification, and a third-party audit confirmed that Alibaba Cloud has indeed established quality management system related documents. In addition, the documentation of Alibaba Cloud's product / service is also available on Alibaba Cloud's official website. |
CCC-03.3: Change Control & Configuration Management - Quality Testing	*Are there policies and procedures in place to triage and remedy reported bugs and security vulnerabilities for product and service offerings?*	Y			是，阿里云已通过ISO9001的认证，并且由三方审计确认阿里云确实建立质量管理体系相关文档	Yes, Alibaba Cloud has passed ISO9001 certification, and a third-party audit confirmed that Alibaba Cloud has indeed established quality management system related documents
CCC-03.4: Change Control & Configuration Management - Quality Testing	*Are mechanisms in place to ensure that all debugging and test code elements are removed from released software versions?*	Y			是，阿里云已通过ISO9001的认证，并且由三方审计确认阿里云确实建立质量管理体系相关文档	Yes, Alibaba Cloud has passed ISO9001 certification, and a third-party audit confirmed that Alibaba Cloud has indeed established quality management system related documents
CCC-04.1: Change Control & Configuration Management - Unauthorized Software Installations	*Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?*	Y			是，未授权软件不得被安装且实时监控，且相应的控制于定期的三方审计过程中也被一并审计确认	Yes, unauthorized software must not be installed and monitored in real time, and the corresponding controls are also audited and confirmed during the regular third-party audit
CCC-05.1: Change Control & Configuration Management - Production Changes	Do you provide tenants with documentation that describes your production change management procedures and their roles/rights / responsibilities within it?	Y			是，在阿里云的SOC报告及安全白皮书内，皆有对客户说明的相应信息	Yes, there are corresponding information explained to customers in Alibaba Cloud's SOC report and security white paper

Data Security and Information Lifecycle Management: Controls DSI-01 through DSI-07

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
DSI-01.1: Data Security & Information Lifecycle Management - Classification	*Do you provide a capability to identify virtual machines via policy tags/metadata (e.g., tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country)?*	Y			是，阿里云云服务器ECS实例是一个虚拟的计算环境，包含CPU、内存、操作系统、磁盘、带宽等最基础的服务器组件，是ECS提供给每个用户的操作实体。一个实例就等同于一台虚拟机，用户对所创建的实例拥有管理员权限，可以随时登录进行使用和管理。	Yes, the ECS instance of Alibaba Cloud Server is a virtual computing environment that contains the most basic server components such as CPU, memory, operating system, disk, and bandwidth. It is an operating instance provided by ECS to each user. An instance is equivalent to a virtual machine. The user has administrator rights to the created instance and can log in to use and manage it at any time.
DSI-01.2: Data Security & Information Lifecycle Management - Classification	*Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (e.g., TXT/TPM, VN-Tag, etc.)?*	Y			是，阿里云通对客户提供ECS实例打标能力	Yes, Alibaba Cloud provides ECS instance marking capabilities to customers
DSI-01.3: Data Security & Information Lifecycle Management - Classification	Do you have a capability to use system geographic location as an authentication factor?	Y			是，阿里云提供了基于IP地址的用户访问控制能力，客户也能够对他们的用户使用阿里云的产品进行基于IP地址的访问控制。	Yes, Alibaba Cloud provides IP address-based user access control capabilities, and customers can also perform IP address-based access control on their users using Alibaba Cloud products.
DSI-01.4: Data Security & Information Lifecycle Management - Classification	*Can you provide the physical location/geography of storage of a tenant's data upon request?*	Y			是，阿里云给客户提供了选择产品所在地域的能力，由客户自行决定其数据存储的地点。	Yes, Alibaba Cloud provides customers with the ability to choose the location of the product, and the customer decides where to store its data.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
DSI-01.5: Data Security & Information Lifecycle Management - Classification	Can you provide the physical location/geography of storage of a tenant's data in advance?	Y			是，阿里云在产品购买时向客户明示可选择的产品所在地域的清单，如ECS产品的地域和可用区情况见https://help.aliyun.com/document_detail/123712.html	Yes, Alibaba Cloud clearly indicates to customers the list of product locations that can be selected when purchasing products. For example, the region and availability of ECS products can be found at https://help.aliyun.com/document_detail/123712.html
DSI-01.6: Data Security & Information Lifecycle Management - Classification	*Do you follow a structured data- labeling standard (e.g., ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?*	Y			是，客户对其数据进行安全管控，依据其业务需求进行数据的标识操作。	Yes, customers manage their data securely, and perform data identification operations based on their business needs.
DSI-01.7: Data Security & Information Lifecycle Management - Classification	*Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?*	Y			是，阿里云给客户提供了选择产品所在地域的能力，由客户自行决定其数据存储的地点。	Yes, Alibaba Cloud provides customers with the ability to choose the location of the product, and the customer decides where to store its data.
DSI-02.1: Data Security & Information Lifecycle Management - Data Inventory/Flows	*Do you inventory, document, and maintain data flows for data that is resident (permanent or temporary) within the services' applications and infrastructure network and systems?*	Y			是，阿里云对所有的网络数据流量均进行了记录。	Yes, Alibaba Cloud has recorded all network data traffic.
DSI-02.2: Data Security & Information Lifecycle Management - Data Inventory/Flows	*Can you ensure that data does not migrate beyond a defined geographical residency?*	Y			是，阿里云给客户提供了选择产品所在地域的能力，由客户自行决定其数据存储的地点。	Yes, Alibaba Cloud provides customers with the ability to choose the location of the product, and the customer decides where to store its data.
DSI-03.1: Data Security & Information Lifecycle Management - e-Commerce Transactions	*Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)?*	Y			是，阿里云在云产品中支持使用开放加密算法，详见阿里云安全白皮书 https://security.aliyun.com/trust	Yes, Alibaba Cloud supports the use of open encryption algorithms in cloud products. For details, see Alibaba Cloud Security White Paper https://security.aliyun.com/trust
DSI-03.2: Data Security & Information Lifecycle Management - e-Commerce Transactions	*Do you utilize open encryption methodologies any time your infrastructure components need to communicate with each other via public networks (e.g., Internet- based replication of data from one environment to another)?*	Y			是，阿里云产品为用户访问（包括读取和上传）数据提供了SSL/TLS协议来保证数据传输的安全。例如，用户如果通过阿里云控制台操作，阿里云控制台会使用HTTPS进行数据传输。所有的阿里云产品都为客户提供了支持HTTPS的API访问点，并提供高达256位密钥的传输加密强度，满足敏感数据加密传输需求。	Yes, Alibaba Cloud products provide SSL/TLS protocols for users to access (including read and upload) data to ensure the security of data transmission. For example, if the user operates through the Alibaba Cloud console, the Alibaba Cloud console will use HTTPS for data transmission. All Alibaba Cloud products provide customers with API access points that support HTTPS, and provide transmission encryption strength of up to 256-bit keys to meet sensitive data encryption transmission requirements.
DSI-04.1: Data Security & Information Lifecycle Management - Handling/Labeling/Security Policy	*Are policies and procedures established for labeling, handling and the security of data and objects that contain data?*	Y			是，客户存放在云上的数据由客户依据其业务需求和安全策略流程进行管控。	Yes, the data that customers store on the cloud is managed and controlled by customers in accordance with their business needs and security policy processes.
DSI-04.2: Data Security & Information Lifecycle Management - Handling/Labeling/Security Policy	*Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?*	Y			是，客户存放在云上的数据由客户依据其业务需求和安全策略流程进行管控。	Yes, the data that customers store on the cloud is managed and controlled by customers in accordance with their business needs and security policy processes.
DSI-05.1: Data Security & Information Lifecycle Management - Non-Production Data	*Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?*	Y			是，阿里云内部建立了规范的流程以保证非必要场景下不会在非生产环境使用阿里云业务中生产环境的数据，客户的数据由客户根据其数据安全要求进行管控。	Yes, Alibaba Cloud has established a standardized process to ensure that the data in the production environment of Alibaba Cloud's business will not be used in non-production environments in non-essential scenarios. The customer's data is controlled by the customer according to its data security requirements.
DSI-06.1: Data Security & Information Lifecycle Management - Ownership/Stewardship	*Are the responsibilities regarding data stewardship defined, assigned, documented and communicated?*	Y			是，阿里云在相关法律协议条款和安全白皮书中明确说明了阿里云和客户在数据安全上的职责边界。	Yes, Alibaba Cloud clearly states the boundaries of Alibaba Cloud's and customers' data security responsibilities in relevant legal agreement terms and security white papers.
DSI-07.1: Data Security & Information Lifecycle Management - Secure Disposal	*Do you support secure deletion (e.g., degaussing/cryptographic wiping) of archived and backed-up data as determined by the tenant?*	Y			是，阿里云建立了数据安全删除的机制，当面向客户的服务终止时会及时删除云服务客户数据资产或根据相关协议要求返还其数据资产。	Yes, Alibaba Cloud has established a mechanism for secure data deletion. When the customer-facing service is terminated, the cloud service customer's data assets will be deleted in a timely manner or returned to their data assets in accordance with the requirements of relevant agreements.
DSI-07.2: Data Security & Information Lifecycle Management - Secure Disposal	*Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?*	Y			是，阿里云安全白皮书的8.6章节为数据销毁的相关说明。	Yes, section 8.6 of the Alibaba Cloud Security White Paper is related to data destruction security.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
Datacenter Security: Controls DCS-01 through DCS-09						
DCS-01.1: Datacenter Security - Asset Management	*Do you maintain a complete inventory of all of your critical assets that includes ownership of the asset?*	Y			是，阿里云通过电子系统对所有的资产进行管理。	Yes, Alibaba Cloud manages all assets through systems.
DCS-01.2: Datacenter Security - Asset Management	*Do you maintain a complete inventory of all of your critical supplier relationships?*	Y			是，阿里云通过电子系统进行供应商资源管理。	Yes, Alibaba Cloud manages supplier resources through systems.
DCS-02.1: Datacenter Security - Controlled Access Points	*Are physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?*	Y			是，阿里云遵循相关合规资质认证标准中的要求进行物理安全管理，建立了物理安全的系列规章制度、流程，并设立的专门的团队对物理安全机制的控制落实情况进行检查。详见SOC 2/3报告。	Yes, Alibaba Cloud follows the requirements of relevant compliance certification standards for physical security management, establishes a series of rules and procedures for physical security, and sets up a dedicated team to check the implementation of the physical security mechanism control. See the SOC 2/3 report for details.
DCS-03.1: Datacenter Security - Equipment Identification	*Is automated equipment identification used as a method to validate connection authentication integrity based on known equipment location?*	Y			是，阿里云遵循相关合规资质认证标准中的要求进行物理安全管理，建立了物理安全的系列规章制度、流程，并设立的专门的团队对物理安全机制的控制落实请款进行检查。	Yes, Alibaba Cloud complies with the requirements of relevant compliance certification standards for physical security management, establishes a series of rules and procedures for physical security, and sets up a dedicated team to check the control and implementation of the physical security mechanism.
DCS-04.1: Datacenter Security - Off-Site Authorization	*Do you provide tenants with documentation that describes scenarios in which data may be moved from one physical location to another? (e.g., offsite backups, business continuity failovers, replication)*	Y			是，阿里云给客户提供了选择产品所在地域的能力，由客户自行决定其数据存储的地点。	Yes, Alibaba Cloud provides customers with the ability to choose the location of the product, and the customer decides where to store its data.
DCS-05.1: Datacenter Security - Off-Site Equipment	*Can you provide tenants with evidence documenting your policies and procedures governing asset management and repurposing of equipment?*	Y			是，阿里云依循相关国际标准（如ISO27001/CSA-STAR等）建立资产管理流程，包含资产识别、使用、汰换与销毁过程，可通过SOC2/3报告查看相关信息	Yes, Alibaba Cloud establishes asset management processes in accordance with relevant international standards (such as ISO27001/CSA-STAR, etc.), including asset identification, use, replacement and destruction processes. You can view related information through the SOC2/3 report
DCS-06.1: Datacenter Security - Policy	*Can you provide evidence that policies, standards and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?*	Y			是，阿里云依循相关国际标准（如ISO27001/CSA-STAR等）建立机房安全管理流程，可通过SOC2/3报告查看相关信息	Yes, Alibaba Cloud establishes computer room security management processes in accordance with relevant international standards (such as ISO27001/CSA-STAR, etc.), and relevant information can be viewed through SOC2/3 reports
DCS-06.2: Datacenter Security - Policy	*Can you provide evidence that your personnel and involved third parties have been trained regarding your documented policies, standards and procedures?*	Y			是，阿里云对与数据中心运营相关的员工及第三方人员均进行相关的物理安全知识培训。	Yes, Alibaba Cloud provides relevant physical security knowledge training to employees and third-party personnel related to data center operations.
DCS-07.1: Datacenter Security - Secure Area Authorization	*Do you allow tenants to specify which of your geographic locations their data is allowed to move into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?*	Y			是，阿里云给客户提供了选择产品所在地域的能力，由客户自行决定其数据存储的地点。	Yes, Alibaba Cloud provides customers with the ability to choose the location of the product, and the customer decides where to store its data.
DCS-08.1: Datacenter Security - Unauthorized Persons Entry	*Are ingress and egress points, such as service areas and other points where unauthorized personnel may enter the premises, monitored, controlled and isolated from data storage and process?*	Y			是，阿里云数据中心仅向本数据中心运维人员授予长期访问权限，一旦运维人员转岗或离职，权限立即清除。其他人员若因为业务需求要进入数据中心，必须先提出申请，经各方主管审批通过后才能获取短期授权；每次出入需要出示证件并进行登记，且数据中心运维人员全程陪同。阿里云数据中心内部划分机房包间、测电区域、库房间等区域，各个区域拥有独立的门禁系统，重要区域采用指纹等双因素认证，特定区域采用铁笼进行物理隔离。阿里云园区和办公区均设置入口管控并划分单独的访客区，访客出入必须佩戴证件，且由阿里云员工陪同。阿里云数据中心机房各区域设有安防监控系统，监控范围覆盖所有区域和通道，配有物业保安7*24小时巡逻。所有视频监控和文档记录均会长期保存，且由专人定期复核。	Yes, the Alibaba Cloud data center only grants long-term access rights to the operation and maintenance personnel of this data center. Once the operation and maintenance personnel are transferred or resigned, the permissions are immediately cleared. If other personnel want to enter the data center due to business needs, they must first apply for it and obtain short-term authorization after being approved by the supervisors of all parties; each time they enter and exit, they need to show their credentials and register, and the data center operation and maintenance personnel are accompanied throughout the process. The Alibaba Cloud data center is divided into areas such as computer rooms, power areas, and warehouse rooms. Each area has an independent access control system. Important areas use two-factor authentication such as fingerprints. Specific areas use iron cages for physical isolation. Alibaba Cloud Park and the office area are equipped with entrance control and a separate visitor area. Visitors must wear IDs when they enter and exit, and are accompanied by Alibaba Cloud employees. Each area of the Alibaba Cloud data center computer room is equipped with a security monitoring system that covers all areas and aisles, and is equipped with property security patrols 7 * 24 hours. All video surveillance and documentation will be kept for

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
DCS-09.1: Datacenter Security - User Access	*Do you restrict physical access to information assets and functions by users and support personnel?*	Y			是，阿里云数据中心仅向本数据中心运维人员授予长期访问权限，一旦运维人员转岗或离职，权限立即清除。其他人员若因为业务需求要进入数据中心，必须先提出申请，经各方主管审批通过后才能获取短期授权；每次出入需要出示证件并进行登记，且数据中心运维人员全程陪同。阿里云数据中心内部划分机房包间、测电区域、库房间等区域，各个区域拥有独立的门禁系统，重要区域采用指纹等双因素认证，特定区域采用铁笼进行物理隔离。阿里云园区和办公区均设置入口管控并划分单独的访客区，访客出入必须佩戴证件，且由阿里云员工陪同。阿里云数据中心机房各区域均设有安防监控系统，监控范围覆盖所有区域和通道，配有物业保安7*24小时巡逻。所有视频监控和文档记录均会长期保存，且由专人定期复核。	Yes, the Alibaba Cloud data center only grants long-term access rights to the operation and maintenance personnel of this data center. Once the operation and maintenance personnel are transferred or resigned, the permissions are immediately cleared. If other personnel want to enter the data center due to business needs, they must first apply for it and obtain short-term authorization after being approved by the supervisors of all parties; each time they enter and exit, they need to show their credentials and register, and the data center operation and maintenance personnel are accompanied throughout the process. The Alibaba Cloud data center is divided into areas such as computer rooms, power areas, and warehouse rooms. Each area has an independent access control system. Important areas use two-factor authentication such as fingerprints. Specific areas use iron cages for physical isolation. Alibaba Cloud Park and the office area are equipped with entrance control and a separate visitor area. Visitors must wear IDs when they enter and exit, and are accompanied by Alibaba Cloud employees. Each area of the Alibaba Cloud data center computer room is equipped with a security monitoring system that covers all areas and aisles, and is equipped with property security patrols 7 * 24 hours. All video surveillance and documentation will be kept for
Encryption and Key Management: Controls EKM-01 through EKM-04						
EKM-01.1: Encryption & Key Management - Entitlement	*Do you have key management policies binding keys to identifiable owners?*	Y			是，阿里云已建立密钥管理的策略和要求。	Yes, Alibaba Cloud has established policies and requirements for key management.
EKM-02.1: Encryption & Key Management - Key Generation	*Do you have a capability to allow creation of unique encryption keys per tenant?*	Y			是，阿里云云产品的存储加密功能支持使用托管给云产品的服务密钥作为主密钥实现。当用户在一个地域第一次使用某一个云产品服务的数据加密功能时，该服务系统会为用户在密钥管理服务（KMS）中的使用地域自动创建一个专为 该服务使用的用户主密钥（Customer Master Key，简称CMK）。本密钥会作为服务密钥且其生命周期是托管给云产品的。用户可以通过在支持的云产品中选择自己创建或上传用户主密钥（CMK）到KMS中，并直接管理自选密钥的生命周期。	Yes, the storage encryption function of Alibaba Cloud products supports the use of service keys hosted to cloud products as the master key. When a user uses the data encryption function of a certain cloud product service for the first time in a region, the service system will automatically create a user secret for the region where the user uses the key management service (KMS). Customer Master Key (CMK). This key acts as a service key and its life cycle is hosted to the cloud product. Users can choose to create or upload a user master key (CMK) to the KMS by selecting one of the supported cloud products, and directly manage the life cycle of the self-selected key
EKM-02.2: Encryption & Key Management - Key Generation	*Do you have a capability to manage encryption keys on behalf of tenants?*	Y			是，阿里云云产品的存储加密功能支持使用托管给云产品的服务密钥作为主密钥实现。当用户在一个地域第一次使用某一个云产品服务的数据加密功能时，该服务系统会为用户在密钥管理服务（KMS）中的使用地域自动创建一个专为 该服务使用的用户主密钥（Customer Master Key，简称CMK）。本密钥会作为服务密钥且其生命周期是托管给云产品的。用户可以通过在支持的云产品中选择自己创建或上传用户主密钥（CMK）到KMS中，并直接管理自选密钥的生命周期。	Yes, the storage encryption function of Alibaba Cloud products supports the use of service keys hosted to cloud products as the master key. When a user uses the data encryption function of a certain cloud product service for the first time in a region, the service system will automatically create a user secret for the region where the user uses the key management service (KMS). Customer Master Key (CMK). This key acts as a service key and its life cycle is hosted to the cloud product. Users can choose to create or upload a user master key (CMK) to the KMS by selecting one of the supported cloud products, and directly manage the life cycle of the self-selected key
EKM-02.3: Encryption & Key Management - Key Generation	*Do you maintain key management procedures?*	Y			是，阿里云云产品的存储加密功能支持使用托管给云产品的服务密钥作为主密钥实现。当用户在一个地域第一次使用某一个云产品服务的数据加密功能时，该服务系统会为用户在密钥管理服务（KMS）中的使用地域自动创建一个专为 该服务使用的用户主密钥（Customer Master Key，简称CMK）。本密钥会作为服务密钥且其生命周期是托管给云产品的。用户可以通过在支持的云产品中选择自己创建或上传用户主密钥（CMK）到KMS中，并直接管理自选密钥的生命周期。	Yes, the storage encryption function of Alibaba Cloud products supports the use of service keys hosted to cloud products as the master key. When a user uses the data encryption function of a certain cloud product service for the first time in a region, the service system will automatically create a user secret for the region where the user uses the key management service (KMS). Customer Master Key (CMK). This key acts as a service key and its life cycle is hosted to the cloud product. Users can choose to create or upload a user master key (CMK) to the KMS by selecting one of the supported cloud products, and directly manage the life cycle of the self-selected key

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
EKM-02.4: Encryption & Key Management - Key Generation	*Do you have documented ownership for each stage of the lifecycle of encryption keys?*	Y			是，阿里云云产品的存储加密功能支持使用托管给云产品的服务密钥作为主密钥实现。当用户在一个地域第一次使用某一个云产品服务的数据加密功能时，该服务系统会为用户在密钥管理服务（KMS）中的使用地域自动创建一个专为 该服务使用的用户主密钥（Customer Master Key，简称CMK）。本密钥会作为服务密钥且其生命周期是托管给云产品的。用户可以通过在支持的云产品中选择自己创建或上传用户主密钥（CMK）到KMS中，并直接管理自选密钥的生命周期。	Yes, the storage encryption function of Alibaba Cloud products supports the use of service keys hosted to cloud products as the master key. When a user uses the data encryption function of a certain cloud product service for the first time in a region, the service system will automatically create a user secret for the region where the user uses the key management service (KMS). Customer Master Key (CMK). This key acts as a service key and its life cycle is hosted to the cloud product. Users can choose to create or upload a user master key (CMK) to the KMS by selecting one of the supported cloud products, and directly manage the life cycle of the self-selected key
EKM-02.5: Encryption & Key Management - Key Generation	*Do you utilize any third party/open source/proprietary frameworks to manage encryption keys?*	Y			是，阿里云的KMS服务支持用户将密钥托管在硬件安全模块（Hardware Security Module，HSM）之中，并可利用HSM进行密码运算和安全托管等功能。各市场分别符合市场认可的密码合规标准，阿里云的密钥管理服务的系统机制，包含其使用的HSM，也符合PCI-DSS合规。	Yes, Alibaba Cloud's KMS service allows users to host keys in a Hardware Security Module (HSM), and can use HSM for cryptographic operations and secure escrow functions. Each market meets the market-recognized password compliance standards, and the system mechanism of Alibaba Cloud's key management service, including the HSMs it uses, also comply with PCI-DSS compliance.
EKM-03.1: Encryption & Key Management - Sensitive Data Protection	*Do you encrypt tenant data at rest (on disk/storage) within your environment?*	Y			是，阿里云为客户提供了云产品落盘存储加密能力给用户，并统一使用阿里云密钥管理服务（Key Management Service，简称KMS）进行密钥管理。阿里云的存储加密提供256位密钥的存储加密强度（AES256），满足敏感数据的加密存储需求。如EBS、OSS、RDS、TableStore、NAS、Maxcompute,详见阿里云安全白皮书。	Yes, Alibaba Cloud provides customers with cloud storage encryption capabilities for users, and uses Alibaba Cloud Key Management Service (KMS) for key management. Alibaba Cloud's storage encryption provides a storage encryption strength of 256-bit keys (AES256) to meet the encrypted storage needs of sensitive data. Such as EBS, OSS, RDS, TableStore, NAS, Maxcompute, see Alibaba Cloud Security White Paper for details.
EKM-03.2: Encryption & Key Management - Sensitive Data Protection	*Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?*	Y			是，用户如果通过阿里云控制台操作，阿里云控制台会使用HTTPS进行数据传输。所有的阿里云产品都为客户提供了支持HTTPS的API访问点，并提供高达256位密钥的传输加密强度。	Yes, if users operate through Alibaba Cloud console, Alibaba Cloud console will use HTTPS for data transmission. All Alibaba Cloud products provide customers with API access points that support HTTPS, and provide transmission encryption strength of up to 256-bit keys.
EKM-03.3: Encryption & Key Management - Sensitive Data Protection	*Do you support tenant-generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate (e.g., identity-based encryption)?*	Y			是，用户可以通过在支持的云产品中选择自己创建或上传用户主密钥（CMK）到KMS中，并直接管理自选密钥的生命周期。通过RAM的授权后，自选密钥也可用于云产品的数据加密功能，并赋能用户更多的安全能力。	Yes, users can choose to create or upload a Customer Master Key (CMK) to the KMS by choosing among the supported cloud products, and directly manage the life cycle of the self-selected key. After being authorized by the RAM, the optional key can also be used for the data encryption function of cloud products and empower users with more security capabilities.
EKM-03.4: Encryption & Key Management - Sensitive Data Protection	*Do you have documentation establishing and defining your encryption management policies, procedures and guidelines?*	Y			是，阿里云依循相关国际标准（如ISO27001/CSA-STAR等）建立加密管理机制，包含创建、使用、汰换等，可通过SOC2/3报告查看相关信息	Yes, Alibaba Cloud establishes encryption management mechanisms in accordance with relevant international standards (such as ISO27001/CSA-STAR, etc.), including creation, use, and replacement. You can view related information through the SOC2/3 report
EKM-04.1: Encryption & Key Management - Storage and Access	Do you have platform and data appropriate encryption that uses open/validated formats and standard algorithms?	Y			是，阿里云的加密服务全面支持国产算法以及部分国际通用密码算法，满足用户各种加密算法需求。对称密码算法：支持SM1、SM4、DES、3DES、AES；非对称密码算法：支持SM2、RSA（1024-2048）；摘要算法：支持SM3、SHA1、SHA256、SHA384。	Yes, Alibaba Cloud's encryption services fully support domestic algorithms and some international common cryptographic algorithms to meet users' various encryption algorithm needs. Symmetric cipher algorithm: support SM1, SM4, DES, 3DES, AES; asymmetric cipher algorithm: support SM2, RSA (1024-2048); digest algorithm: support SM3, SHA1, SHA256, SHA384.
EKM-04.2: Encryption & Key Management - Storage and Access	*Are your encryption keys maintained by the cloud consumer or a trusted key management provider?*	Y			是，阿里云负责维护自己的加密密钥，同时客户需要负责维护自己的加密密钥	Yes, Alibaba Cloud is responsible for maintaining its own encryption keys, and customers are responsible for maintaining their own encryption keys
EKM-04.3: Encryption & Key Management - Storage and Access	*Do you store encryption keys in the cloud?*	Y			是，阿里云将自己的秘钥存储在生产环境中。	Yes, Alibaba Cloud stores its own keys in a production environment.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
EKM-04.4: Encryption & Key Management - Storage and Access	*Do you have separate key management and key usage duties?*	Y			是，阿里云的密钥管理系统独立于密钥使用的业务。	Yes, Alibaba Cloud's key management system is isolated from the key use business.

Governance and Risk Management: Controls GRM-01 through GRM-11

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
GRM-01.1: Governance and Risk Management - Baseline Requirements	*Do you have documented information security baselines for every component of your infrastructure (e.g., hypervisors, operating systems, routers, DNS servers, etc.)?*	Y			是，阿里云于内部规范已有制定安全基线，针对物理、虚拟及相关元件皆有不同的安全基线要求	Yes, Alibaba Cloud has established a security baseline in its internal requirements. There are different security baseline requirements for physical, virtual, and related components.
GRM-01.2: Governance and Risk Management - Baseline Requirements	*Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?*	Y			是，阿里云通过系统的方式监测相关安全基线的配置与运行状况	Yes, Alibaba Cloud monitors the configuration and operating status of relevant security baselines in a systematic way
GRM-01.3: Governance and Risk Management - Baseline Requirements	*Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?*	Y			是，阿里云提供客户创建或导入自定义镜像的能力	Yes, Alibaba Cloud provides customers with the ability to create or import custom images
GRM-02.1: Governance and Risk Management - Data Focus Risk Assessments	*Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status)?*	Y			是，阿里云提供了云监控产品，让客户可以通过可视化的方式查看资源运行状况	Yes, Alibaba Cloud provides cloud monitoring products, allowing customers to visually check the resource operation status
GRM-02.2: Governance and Risk Management - Data Focus Risk Assessments	*Do you conduct risk assessments associated with data governance requirements at least once a year?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立风险评估流程，并且通过三方的审计确认	Yes, Alibaba Cloud establishes a risk assessment process in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.) and has been confirmed by third-party audits
GRM-03.1: Governance and Risk Management - Management Oversight	*Are your technical, business, and executive managers responsible for maintaining awareness of and compliance with security policies, procedures, and standards for both themselves and their employees as they pertain to the manager and employees' area of responsibility?*	Y			是，阿里云的管理层与相应的权责团队会依照频率要求定期审阅信息安全相应的文档，确保文档的适用与可操作性	Yes, Alibaba Cloud's management and the corresponding rights and responsibilities team will regularly review the information security corresponding documents according to the frequency requirements to ensure the application and operability of the documents
GRM-04.1: Governance and Risk Management - Management Program	*Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?*	Y			是，阿里云提供三方审计报告以及相关认证信息，并且持续遵循ISO27001维护相应文档	Yes, Alibaba Cloud provides third-party audit reports and related certification information, and continues to follow ISO27001 to maintain corresponding documents
GRM-04.2: Governance and Risk Management - Management Program	*Do you review your Information Security Management Program (ISMP) least once a year?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立信息安全管理体系，且至少每年审阅一次	Yes, Alibaba Cloud establishes an information security management system in accordance with relevant international standards (such as ISO27001), and reviews it at least once a year
GRM-05.1: Governance and Risk Management - Management Support/Involvement	*Do you ensure your providers adhere to your information security and privacy policies?*	Y			是，阿里云在供应商管理流程内已纳入安全与隐私相关的要求，且在双方的合同内纳入相应管理要求，确保供应商必须遵循相关的要求	Yes, Alibaba Cloud has included security and privacy related requirements in the supplier management process, and included the corresponding management requirements in the contract between the two parties to ensure that the supplier must comply with the relevant requirements
GRM-06.1: Governance and Risk Management - Policy	*Do your information security and privacy policies align with industry standards (ISO- 27001, ISO-22307, CoBIT, etc.)?*	Y			是，阿里云依循相关国际标准（ISO27001/27017/27018/27701等）建立信息安全与隐私管理体系	Yes, Alibaba Cloud establishes an information security and privacy management system in accordance with relevant international standards (ISO27001/27017/27018/27701, etc.)
GRM-06.2: Governance and Risk Management - Policy	*Do you have agreements to ensure your providers adhere to your information security and privacy policies?*	Y			是，阿里云在供应商管理流程内已纳入安全与隐私相关的要求，且在双方的合同内纳入相应管理要求，确保供应商必须遵循相关的要求	Yes, Alibaba Cloud has included security and privacy related requirements in the supplier management process, and included the corresponding management requirements in the contract between the two parties to ensure that the supplier must comply with the relevant requirements
GRM-06.3: Governance and Risk Management - Policy	*Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?*	Y			是，阿里云提供SOC2/3报告作为内部控制与AICPA TSC标准的映射信息	Yes, Alibaba Cloud provides SOC2/3 report as mapping information between internal control and AICPA TSC standard
GRM-06.4: Governance and Risk Management - Policy	*Do you disclose which controls, standards, certifications and/or regulations you comply with?*	Y			是，阿里云持续完成多个国际标准、行业认证的要求，并展示于阿里云信任中心	Yes, Alibaba Cloud has continuously completed multiple international standards and industry certification requirements, and displayed it at Alibaba Cloud Trust Center
GRM-07.1: Governance and Risk Management - Policy Enforcement	*Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?*	Y			是，阿里云在员工管理的举措中，包含对于人员行为规范与安全红线的处置方式	Yes, Alibaba Cloud's measures for employee management include the disposal of personnel behavior standards and safety redlines

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
GRM-07.2: Governance and Risk Management - Policy Enforcement	*Are employees made aware of what actions could be taken in the event of a violation via their policies and procedures?*	Y			是，所有员工在入职时，都必须完成员工管理相关的守则阅读与确认	Yes, all employees must complete the relevant employee management code of conduct reading and confirmation upon entry
GRM-08.1: Governance and Risk Management - Policy Impact on Risk Assessments	*Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立风险评估流程，并且将风险评估结果纳入体系持续优化的输入	Yes, Alibaba Cloud establishes a risk assessment process in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.), and incorporates the risk assessment results into the input of the system's continuous optimization
GRM-09.1: Governance and Risk Management - Policy	*Do you notify your tenants when you make material changes to your information security and/or privacy policies?*	Y			是，虽信息安全相关管理体系属于阿里云内部信息，但若有影响客户时，也会同步于安全白皮书内更新	Yes, although the information security related management system belongs to Alibaba Cloud internal information, if it affects customers, it will also be updated in the security white paper.
GRM-09.2: Governance and Risk Management - Policy	*Do you perform, at minimum, annual reviews to your privacy and security policies?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立信息安全管理体系，且至少每年审阅一次	Yes, Alibaba Cloud establishes an information security management system in accordance with relevant international standards (such as ISO27001), and reviews it at least once a year
GRM-10.1: Governance and Risk Management - Risk Assessments	*Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立风险评估流程，并且通过三方的审计确认	Yes, Alibaba Cloud establishes a risk assessment process in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.) and has been confirmed by third-party audits
GRM-10.2: Governance and Risk Management - Risk Assessments	*Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立风险评估流程，并且通过三方的审计确认	Yes, Alibaba Cloud establishes a risk assessment process in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.) and has been confirmed by third-party audits
GRM-11.1: Governance and Risk Management - Management Framework	*Do you have a documented, organization-wide program in plcae to manage risk?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立风险评估流程，并记录与跟进相关的风险处置方案	Yes, Alibaba Cloud establishes a risk assessment process in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.) and has been confirmed by third-party audits
GRM-11.2: Governance and Risk Management - Management Framework	*Do you make available documentation of your organization-wide risk management program?*	Y			是，阿里云依循相关国际标准（如ISO9001/27001/27017/27018等）建立风险评估流程，并记录与跟进相关的风险处置方案	Yes, Alibaba Cloud establishes a risk assessment process in accordance with relevant international standards (such as ISO9001/27001/27017/27018, etc.) and has been confirmed by third-party audits

Human Resources: Controls HRS-01 through HRS-11

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
HRS-01.1: Human Resources - Asset Returns	*Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?*	Y			是，阿里云建立了隐私泄露的应急响应流程，当涉及客户的隐私泄漏时将向客户明确告知。	Yes, Alibaba Cloud has established an emergency response process for privacy breach, and will clearly inform customers when it involves customer privacy breach.
HRS-01.2: Human Resources - Asset Returns	*Is your Privacy Policy aligned with industry standards?*	Y			是，阿里云的隐私权政策符合行业相关标准，目前阿里云已经获得了隐私领域的ISO 27701/27018/29151 和BS 10012认证。	Yes, Alibaba Cloud's privacy policy complies with relevant industry standards. At present, Alibaba Cloud has obtained ISO 27701/27018/29151 and BS 10012 certifications in the field of privacy.
HRS-02.1: Human Resources - Background Screening	*Pursuant to local laws, regulations, ethics and contractual constraints, are all employment candidates, contractors and involved third parties subject to background verification?*	Y			是，阿里云会依据行业最佳实践开展对员工及第三方的背景调查。	Yes, Alibaba Cloud conducts background checks on employees and third parties based on industry best practices.
HRS-03.1: Human Resources - Employment Agreements	*Do you specifically train your employees regarding their specific role and the information security controls they must fulfill?*	Y			是，阿里云针对员工整体的安全意识及职业技能均会展开定期的培训。	Yes, Alibaba Cloud conducts regular training for employees' overall security awareness and professional skills.
HRS-03.2: Human Resources - Employment Agreements	*Do you document employee acknowledgment of training they have completed?*	Y			是，阿里云开展的员工培训均会有相关的培训记录或考试记录。	Yes, all employee training conducted by Alibaba Cloud will have related training records or examination records.
HRS-03.3: Human Resources - Employment Agreements	*Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information?*	Y			是，阿里云所有的员工入职均需签署标准模板的保密协议。	Yes, all employees of Alibaba Cloud must sign a non-disclosure agreement with a standard template for entry.
HRS-03.4: Human Resources - Employment Agreements	*Is successful and timed completion of the training program considered a prerequisite for acquiring and maintaining access to sensitive systems?*	Y			是，阿里云将新员工入职培训及年度的培训作为每个员工必须完成的工作任务。	Yes, Alibaba Cloud takes new employee induction training and annual training as a task that each employee must complete.
HRS-03.5: Human Resources - Employment Agreements	*Are personnel trained and provided with awareness programs at least once a year?*	Y			是，阿里云每年都会启动对员工的安全意识培训。	Yes, Alibaba Cloud launches security awareness training for employees every year.
HRS-04.1: Human Resources - Employment Termination	Are documented policies, procedures and guidelines in place to govern change in employment and/or termination?	Y			是，阿里云建立了员工入职、装转岗和离职的管控流程，将员工的账号权限管理与HR流程自动化打通。	Yes, Alibaba Cloud has established management and control procedures for employees' on-boarding, transfer, and resignation to automate the management of employee account rights and HR processes.
HRS-04.2: Human Resources - Employment Termination	*Do the above procedures and guidelines account for timely revocation of access and return of assets?*	Y			是，阿里云建立了员工入职、装转岗和离职的管控流程，将员工的账号权限管理与HR流程自动化打通。	Yes, Alibaba Cloud has established management and control procedures for employees' on-boarding, transfer, and resignation to automate the management of employee account rights and HR processes.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
HRS-05.1: Human Resources - Mobile Device Management	*Are policies and procedures established and measures implemented to strictly limit access to your sensitive data and tenant data from portable and mobile devices (e.g., laptops, cell phones and personal digital assistants (PDAs)), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?*	Y			是，阿里云严格管控员工工作中终端设备安全，非授权设备不可进入办公内网。阿里云不会在未授权状况下触碰用户数据。	Yes, Alibaba Cloud strictly controls the security of terminal equipment during employees' work. Unauthorized equipment cannot enter the office intranet. Alibaba Cloud will not access user data without authorization.
HRS-06.1: Human Resources - Non-Disclosure Agreements	*Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?*	Y			是，阿里云会定期审阅保密协议文件以保证适应业务的需求。	Yes, Alibaba Cloud regularly reviews the confidentiality agreement documents to ensure that they meet the needs of the business.
HRS-07.1: Human Resources - Roles/Responsibilities	*Do you provide tenants with a role definition document clarifying your administrative responsibilities versus those of the tenant?*	Y			是的，阿里云的安全白皮书中明确说明了与客户的安全管理责任。https://security.aliyun.com/trust	Yes, Alibaba Cloud's security white paper clearly states the security management responsibilities with customers. https://www.alibabacloud.com/trust-center
HRS-08.1: Human Resources - Technology Acceptable Use	*Do you provide documentation regarding how you may or access tenant data and metadata?*	Y			是，阿里云内部建立了访问控制的相关流程机制，遵循最小化原则来进行权限的管控；客户管控对其数据的访问控制，且阿里云不会未授权状况下触碰用户数据。。阿里云整体已通过第三方的ISO27001和ISO 27018的认证。	Yes, Alibaba Cloud has established a related process mechanism for access control, which controls permissions based on the principle of minimization; customers control access to their data, and Alibaba Cloud does not access user data under unauthorized conditions. . Alibaba Cloud has passed ISO27001 and ISO 27018 certifications by third parties.
HRS-08.2: Human Resources - Technology Acceptable Use	*Do you collect or create metadata about tenant data usage through inspection technologies (search engines, etc.)?*			NA	不适用，阿里云不通过这种方式采集数据。	Not applicable, Alibaba Cloud does not collect data in this way.
HRS-08.3: Human Resources - Technology Acceptable Use	*Do you allow tenants to opt out of having their data/metadata accessed via inspection technologies?*			NA	不适用，阿里云不通过这种方式采集数据。	Not applicable, Alibaba Cloud does not collect data in this way.
HRS-09.1: Human Resources - Training/Awareness	*Do you provide a formal, role-based, security awareness training program for cloud-related access and data management issues (e.g., multi-tenancy, nationality, cloud delivery model segregation of duties implications and conflicts of interest) for all persons with access to tenant data?*	Y			是，阿里云开展定期的全员安全意识培训及考试。	Yes, Alibaba Cloud conducts regular security awareness training and examinations for all employees.
HRS-09.2: Human Resources - Traninig/Awareness	*Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?*	Y			是，阿里云开展定期的全员安全意识培训及考试。	Yes, Alibaba Cloud conducts regular security awareness training and examinations for all employees.
HRS-10.1: Human Resources - User Responsibility	*Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?*	Y			是，阿里云开展定期的全员安全意识培训及考试。	Yes, Alibaba Cloud conducts regular security awareness training and examinations for all employees.
HRS-10.2: Human Resources - User Responsiblility	*Are users made aware of their responsibilities for maintaining a safe and secure working environment?*	Y			是，阿里云开展定期的全员安全意识培训及考试。	Yes, Alibaba Cloud conducts regular security awareness training and examinations for all employees.
HRS-10.3: Human Resources - User Responsiblility Human	*Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?*	Y			是，阿里云开展定期的全员安全意识培训及考试。	Yes, Alibaba Cloud conducts regular security awareness training and examinations for all employees.
HRS-11.1: Human Resources - Workspace	*Do your data management policies and procedures address tenant and service level conflicts of interests?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立数据安全管理体系，并通过了三方认证。	Yes, Alibaba Cloud has established a data security management system in accordance with relevant international standards (such as ISO27001/27017/27018, etc.) and has passed third-party certification.
HRS-11.2: Human Resources - Workspace	*Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立数据安全管理体系，并通过了三方认证。	Yes, Alibaba Cloud has established a data security management system in accordance with relevant international standards (such as ISO27001/27017/27018, etc.) and has passed third-party certification.
HRS-11.3: Human Resources - Workspace	*Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?*	Y			是，阿里云支持虚拟机层面的逃逸检测。	Yes, Alibaba Cloud supports escape detection at the virtual machine level.

Identity and Access Management: Controls IAM-01 through IAM-13

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IAM-01.1: Identity & Access Management - Audit Tools Access	*Do you restrict, log and monitor access to your information security management systems? (E.g., hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IAM-01.2: Identity & Access Management - Audit Tools Access	*Do you monitor and log privileged access (administrator level) to information security management systems?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-02.1: Identity & Access Management - Credential Lifecycle/Provision Management	*Do you have controls in place ensuring timely removal of systems access that is no longer required for business purposes?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-02.2: Identity & Access Management - Credential Lifecycle/Provision Management	*Do you provide metrics to track the speed with which you are able to remove systems access that is no longer required for business purposes?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-03.1: Identity & Access Management - Diagnostic/Configuration Ports Access	*Do you use dedicated secure networks to provide management access to your cloud service infrastructure?*	Y			是，阿里云的生产环境、运维环境与办公环境皆有配置网络隔离机制	Yes, Alibaba Cloud's production environment, operation and maintenance environment and office environment all have a network isolation mechanism.
IAM-04.1: Identity & Access Management - Policies and Procedures	*Do you manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access?*	Y			是，阿里云已建立集中的访问管理系统	Yes, Alibaba Cloud has established a centralized access management system
IAM-04.2: Identity & Access Management - Policies and Procedures	*Do you manage and store the user identity of all personnel who have network access, including their level of access?*	Y			是，阿里云已建立集中的访问管理系统	Yes, Alibaba Cloud has established a centralized access management system
IAM-05.1: Identity & Access Management - Segregation of Duties	*Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?*	Y			是，阿里云在安全白皮书内与SOC 2/3审计报告内已有说明相应的信息	Yes, Alibaba Cloud has stated the corresponding information in the security white paper and SOC 2/3 audit report.
IAM-06.1: Identity & Access Management - Source Code Access Restriction	*Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-06.2: Identity & Access Management - Source Code Access Restriction	*Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-07.1: Identity & Access Management - Third Party Access	*Do you provide multi-failure disaster recovery capability?*	Y			是，阿里云依循相关国际标准（ISO27001/22301等）建立业务连续性管理机制，且阿里云提供客户多个可用区的选择，支持客户在多点部署相应的资源，确保服务持续运作。	Yes, Alibaba Cloud establishes a business continuity management mechanism in accordance with relevant international standards (ISO27001/22301, etc.), and Alibaba Cloud provides customers with the choice of multiple Availability Zones, supports customers to deploy corresponding resources at multiple points, and ensures the continuous operation of services.
IAM-07.2: Identity & Access Management - Third Party Access	*Do you monitor service continuity with upstream providers in the event of provider failure?*	Y			是，阿里云依循相关国际标准（ISO27001/22301等）建立业务连续性管理机制，且阿里云提供客户多个可用区的选择，支持客户在多点部署相应的资源，确保服务持续运作。	Yes, Alibaba Cloud establishes a business continuity management mechanism in accordance with relevant international standards (ISO27001/22301, etc.), and Alibaba Cloud provides customers with the choice of multiple Availability Zones, supports customers to deploy corresponding resources at multiple points, and ensures the continuous operation of services.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IAM-07.3: Identity & Access Management - Third Party Access	*Do you have more than one provider for each service you depend on?*	Y			是，阿里云依循相关国际标准（ISO27001/22301等）建立业务连续性管理机制，且阿里云提供客户多个可用区的选择，支持客户在多点部署相应的资源，确保服务持续运作。	Yes, Alibaba Cloud establishes a business continuity management mechanism in accordance with relevant international standards (ISO27001/22301, etc.), and Alibaba Cloud provides customers with the choice of multiple Availability Zones, supports customers to deploy corresponding resources at multiple points, and ensures the continuous operation of services.
IAM-07.4: Identity & Access Management - Third Party Access	*Do you provide access to operational redundancy and continuity summaries, including the services you depend on?*	Y			是，阿里云依循相关国际标准（ISO27001/22301等）建立业务连续性管理机制，且阿里云提供客户多个可用区的选择，支持客户在多点部署相应的资源，确保服务持续运作。	Yes, Alibaba Cloud establishes a business continuity management mechanism in accordance with relevant international standards (ISO27001/22301, etc.), and Alibaba Cloud provides customers with the choice of multiple Availability Zones, supports customers to deploy corresponding resources at multiple points, and ensures the continuous operation of services.
IAM-07.5: Identity & Access Management - Third Party Access	*Do you provide the tenant the ability to declare a disaster?*	Y			是，阿里云依循相关国际标准（ISO27001/22301等）建立业务连续性管理机制，且阿里云提供客户多个可用区的选择，支持客户在多点部署相应的资源，确保服务持续运作。	Yes, Alibaba Cloud establishes a business continuity management mechanism in accordance with relevant international standards (ISO27001/22301, etc.), and Alibaba Cloud provides customers with the choice of multiple Availability Zones, supports customers to deploy corresponding resources at multiple points, and ensures the continuous operation of services.
IAM-07.6: Identity & Access Management - Third Party Access	*Do you provide a tenant-triggered failover option?*	Y			是，阿里云依循相关国际标准（ISO27001/22301等）建立业务连续性管理机制，且阿里云提供客户多个可用区的选择，支持客户在多点部署相应的资源，确保服务持续运作。	Yes, Alibaba Cloud establishes a business continuity management mechanism in accordance with relevant international standards (ISO27001/22301, etc.), and Alibaba Cloud provides customers with the choice of multiple Availability Zones, supports customers to deploy corresponding resources at multiple points, and ensures the continuous operation of services.
IAM-07.7: Identity & Access Management - Third Party Access	*Do you share your business continuity and redundancy plans with your tenants?*		N		否，业务连续性计划属于阿里云内部信息，但定期由三方审计进行审计与确认	No, the business continuity plan belongs to Alibaba Cloud internal information, but is regularly audited and checked by a third-party audit
IAM-08.1: Identity & Access Management - Trusted Sources	*Do you document how you grant and approve access to tenant data?*	Y			是，阿里云于服务协议内说明对于客户数据的管理责任与访问权责，仅在客户授权的状况下才能访问客户数据，且相应的操作都会留存日志以供查验	Yes, Alibaba Cloud stated in the service agreement the management responsibilities and access rights for customer data. The customer data can be accessed only when authorized by the customer, and the corresponding operations will keep logs for inspection.
IAM-08.2: Identity & Access Management - Trusted Sources	*Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?*		N		否，客户数据的分类由客户自身决定	No, the classification of customer data is up to the customer
IAM-09.1: Identity & Access Management - User Access Authorization	*Does your management provision the authorization and restrictions for user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) prior to their access to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-09.2: Identity & Access Management - User Access Authorization	*Do you provide upon request user access (e.g., employees, contractors, customers (tenants), business partners and/or suppliers) to data and any owned or managed (physical and virtual) applications, infrastructure systems and network components?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-10.1: Identity & Access Management - User Access Reviews	*Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-10.2: Identity & Access Management - User Access Reviews	*If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IAM-10.3: Identity & Access Management - User Access Reviews	*Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查。此外，阿里云仅在获得客户授权的情况下才会访问客户的数据，相关权限均遵循统一的访问控制规则。	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation. In addition, Alibaba Cloud only accesses customer data if authorized by the customer, and the relevant permissions follow uniform access control rules.
IAM-11.1: Identity & Access Management - User Access Revocation	*Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or involved third parties?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-11.2: Identity & Access Management - User Access Revocation	*Is any change in user access status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?*	Y			是，阿里云依循相关国际标准（如ISO27001）建立访问控制管理流程，确保访问权限最小化使用，并且通过自动化访问控管机制，确保权限及时收回与冻结，且留存相关日志以供调查	Yes, Alibaba Cloud establishes access control management processes in accordance with relevant international standards (such as ISO27001) to ensure that access rights are minimized, and through automated access control mechanisms, rights are recovered and frozen in a timely manner, and relevant logs are retained for investigation
IAM-12.1: Identity & Access Management - User ID Credentials	*Do you support use of, or integration with, existing customer- based Single Sign On (SSO) solutions to your service?*	Y			是，阿里云的资源访问管理服务支持SSO的集成	Yes, Alibaba Cloud's resource access management service supports SSO integration
IAM-12.2: Identity & Access Management - User ID Credentials	*Do you use open standards to delegate authentication capabilities to your tenants?*	Y			是，阿里云支持SAML 2.0与相关行业通用标准	Yes, Alibaba Cloud supports SAML 2.0 and related industry common standards
IAM-12.3: Identity & Access Management - User ID Credentials	*Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/aut horizing users?*	Y			是，阿里云支持SAML 2.0与相关行业通用标准	Yes, Alibaba Cloud supports SAML 2.0 and related industry common standards
IAM-12.4: Identity & Access Management - User ID Credentials	*Do you have a Policy Enforcement Point capability (e.g., XACML) to enforce regional legal and policy constraints on user access?*	Y			是，阿里云的资源访问管理服务提供权限管理功能，让客户能依照自身的要求配置相关的权限，并且可设置相关的安全功能（如密码复杂度与多因素验证）	Yes, Alibaba Cloud's resource access management service provides permission management functions, allowing customers to configure related permissions according to their own requirements, and can set related security functions (such as password complexity and multi-factor authentication)
IAM-12.5: Identity & Access Management - User ID Credentials	*Do you have an identity management system (enabling classification of data for a tenant) in place to enable both role-based and context-based entitlement to data?*	Y			是，阿里云的资源访问管理服务提供权限管理功能，让客户能依照自身的要求配置相关的权限，并且可设置相关的安全功能（如密码复杂度与多因素验证）	Yes, Alibaba Cloud's resource access management service provides permission management functions, allowing customers to configure related permissions according to their own requirements, and can set related security functions (such as password complexity and multi-factor authentication)
IAM-12.6: Identity & Access Management - User ID Credentials	*Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometrics, etc.) for user access?*	Y			是，阿里云的资源访问管理服务提供权限管理功能，让客户能依照自身的要求配置相关的权限，并且可设置相关的安全功能（如密码复杂度与多因素验证）	Yes, Alibaba Cloud's resource access management service provides permission management functions, allowing customers to configure related permissions according to their own requirements, and can set related security functions (such as password complexity and multi-factor authentication)
IAM-12.7: Identity & Access Management - User ID Credentials	*Do you allow tenants to use third-party identity assurance services?*	Y			是，阿里云的资源访问管理服务提供权限管理功能，让客户能依照自身的要求配置相关的权限，并且可设置相关的安全功能（如密码复杂度与多因素验证）	Yes, Alibaba Cloud's resource access management service provides permission management functions, allowing customers to configure related permissions according to their own requirements, and can set related security functions (such as password complexity and multi-factor authentication)
IAM-12.8: Identity & Access Management - User ID Credentials	*Do you support password (minimum length, age, history, complexity) and account lockout (lockout threshold, lockout duration) policy enforcement?*	Y			是，阿里云的资源访问管理服务提供权限管理功能，让客户能依照自身的要求配置相关的权限，并且可设置相关的安全功能（如密码复杂度与多因素验证）	Yes, Alibaba Cloud's resource access management service provides permission management functions, allowing customers to configure related permissions according to their own requirements, and can set related security functions (such as password complexity and multi-factor authentication)
IAM-12.9: Identity & Access Management - User ID Credentials	*Do you allow tenants/customers to define password and account lockout policies for their accounts?*	Y			是，阿里云的资源访问管理服务提供权限管理功能，让客户能依照自身的要求配置相关的权限，并且可设置相关的安全功能（如密码复杂度与多因素验证）	Yes, Alibaba Cloud's resource access management service provides permission management functions, allowing customers to configure related permissions according to their own requirements, and can set related security functions (such as password complexity and multi-factor authentication)

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IAM-12.10: Identity & Access Management - User ID Credentials	*Do you support the ability to force password changes upon first logon?*	Y			是，阿里云的资源访问管理服务提供权限管理功能，让客户能依照自身的要求配置相关的权限，并且可设置相关的安全功能（如密码复杂度与多因素验证）	Yes, Alibaba Cloud's resource access management service provides permission management functions, allowing customers to configure related permissions according to their own requirements, and can set related security functions (such as password complexity and multi-factor authentication)
IAM-12.11: Identity & Access Management - User ID Credentials	*Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-service via email, defined challenge questions, manual unlock)?*	Y			是，阿里云的资源访问管理服务提供权限管理功能，让客户能依照自身的要求配置相关的权限，并且可设置相关的安全功能（如密码复杂度与多因素验证）	Yes, Alibaba Cloud's resource access management service provides permission management functions, allowing customers to configure related permissions according to their own requirements, and can set related security functions (such as password complexity and multi-factor authentication)
IAM-13.1: Identity & Access Management - Utility Programs Access	*Are utilities that can significantly manage virtualized partitions (e.g., shutdown, clone, etc.) appropriately restricted and monitored?*	Y			是，阿里云的云产品运维系统有划分高危操作，并且确保只有被授权的人员才可能被授予高权限能力	Yes, Alibaba Cloud's cloud product operation and maintenance system is divided into high-risk operations and ensures that only authorized personnel can be granted high authority capabilities
IAM-13.2: Identity & Access Management - Utility Programs Access	*Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shimming, Blue Pill, Hyper jumping, etc.)?*	Y			是，阿里云实时的对云平台进行安全监控，分析潜在的攻击与漏洞，并进行相应的处置	Yes, Alibaba Cloud monitors the cloud platform in real time, analyzes potential attacks and vulnerabilities, and handles them accordingly.
IAM-13.3: Identity & Access Management - Utility Programs Access	*Are attacks that target the virtual infrastructure prevented with technical controls?*	Y			是，阿里云实时的对云平台进行安全监控，分析潜在的攻击与漏洞，并进行相应的处置	Yes, Alibaba Cloud monitors the cloud platform in real time, analyzes potential attacks and vulnerabilities, and handles them accordingly.

Infrastructure and Virtualization Security: Controls IVS-01 through IVS-13

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IVS-01.1: Infrastructure & Virtualization Security - Audit Logging/Intrusion Detection	*Are file integrity (host) and network Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?*	Y			是，阿里云云平台侧的安全监控可及时发现平台自身的应用和主机、网络等资源被恶意攻击的安全事件，并在发现安全事件之后，触发云平台内部应急响应流程进行妥善处置，及时消除影响。	Yes, security monitoring on the Alibaba Cloud platform side can timely discover security incidents in which the platform's own applications and hosts, networks, and other resources have been maliciously attacked. After the security incidents are discovered, the cloud platform's internal emergency response process is triggered to properly handle and eliminate the impact in a timely manner. .
IVS-01.2: Infrastructure & Virtualization Security - Audit Logging/Intrusion Detection	*Is physical and logical user access to audit logs restricted to authorized personnel?*	Y			是，阿里云内部建立了严格的访问控制机制，对日志数据的访问也需遵循访问控制要求。	Yes, Alibaba Cloud has established a strict access control mechanism, and access to log data must also comply with access control requirements.
IVS-01.3: Infrastructure & Virtualization Security - Audit Logging/Intrusion Detection	*Can you provide evidence that due diligence mapping of regulations and standards to your controls/architectu re/processes has been done?*	Y			是，阿里云已经安全控制和相关外部合规要求进行了匹配，如SOC 2/3、ISO 27002等。	Yes, Alibaba Cloud has matched security controls and related external compliance requirements, such as SOC 2/3, ISO 27002, etc.
IVS-01.4: Infrastructure & Virtualization Security - Audit Logging/Intrusion Detection	*Are audit logs centrally stored and retained?*	Y			是，阿里云自动采集日志、集中化管理、实时/准实时监控/审计。	Yes, Alibaba Cloud automatically collects logs, centralized management, and real-time/near-real-time monitoring/auditing.
IVS-01.5: Infrastructure & Virtualization Security - Audit Logging/Intrusion Detection	*Are audit logs reviewed on a regular basis for security events (e.g., with automated tools)?*	Y			是，阿里云自动采集日志、集中化管理、实时/准实时监控/审计。	Yes, Alibaba Cloud automatically collects logs, centralized management, and real-time/near-real-time monitoring/auditing.
IVS-02.1: Infrastructure & Virtualization Security - Change Detection	*Do you log and alert any changes made to virtual machine images regardless of their running state (e.g., dormant, off or running)?*	Y			是，阿里云记录所有的变更，变更日志会纳入日志监控的范围。	Yes, Alibaba Cloud records all changes, and the change log will be included in the scope of log monitoring.
IVS-02.2: Infrastructure & Virtualization Security - Change Detection	*Are changes made to virtual machines, or moving of an image and subsequent validation of the image's integrity, made immediately available to customers through electronic methods (e.q., portals or alerts)?*	Y			是，当阿里云的镜像有更新时，客户可以在官网产品文档或通知内获取相关信息	Yes, when the Alibaba Cloud image is updated, customers can obtain relevant information in the official website product documentation or notification
IVS-03.1: Infrastructure & Virtualization Security - Clock Synchronization	*Do you use a synchronized time- service protocol (e.g., NTP) to ensure all systems have a common time reference?*	Y			是，阿里云已实现了时钟同步。	Yes, Alibaba Cloud has achieved clock synchronization.
IVS-04.1: Infrastructure & Virtualization Security - Information System Documentation	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	Y			是的，阿里云产品均提供了面向客户的SLA文档。	Yes, all Alibaba Cloud products provide customer-oriented SLA documents.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IVS-04.2: Infrastructure & Virtualization Security - Information System Documentation	*Do you restrict use of the memory oversubscriptioncapabilities present in the hypervisor?*	Y			是，阿里云建立了完善的资源管理机制，提前进行容量规划、并系统化的方式对资源进行实时监控，以保证资源对业务需求的满足。	Yes, Alibaba Cloud has established a comprehensive resource management mechanism that performs capacity planning in advance and systematically monitors resources in real time to ensure that resources meet business needs.
IVS-04.3: Infrastructure & Virtualization Security - Information System Documentation	*Do your system capacity requirements take into account current, projected and anticipated capacity needs forall systems used to provide services to the tenants?*	Y			是，阿里云建立了完善的资源管理机制，提前进行容量规划、并系统化的方式对资源进行实时监控，以保证资源对业务需求的满足。	Yes, Alibaba Cloud has established a comprehensive resource management mechanism that performs capacity planning in advance and systematically monitors resources in real time to ensure that resources meet business needs.
IVS-04.4: Infrastructure & Virtualization Security - Information System Documentation	*Is system performance monitored and tuned in order to continuously meet regulatory, contractual and business requirements for all the systems used to provide services to the tenants?*	Y			是，阿里云实施监控各产品的性能以保证对SLA的符合度以及对业务需求和监管需求的符合度。	Yes, Alibaba Cloud monitors the performance of various products to ensure compliance with SLAs and compliance with business and regulatory requirements.
IVS-05.1: Infrastructure & Virtualization Security - Vulnerability Management	*Do security vulnerability assessment tools or services accommodate the virtualization technologies being used (e.g., virtualization aware)?*	Y			是，阿里云采用漏洞扫描、渗透测试、黑盒/白盒测试等形式来发现安全问题。	Yes, Alibaba Cloud uses vulnerability scanning, penetration testing, and black/white box testing to discover security issues.
IVS-06.1: Infrastructure & Virtualization Security - Network Security	*For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?*	Y			是，阿里云发布了安全白皮书、企业上云安全指引等指引类文件帮助用户实现产品的安全部署。	Yes, Alibaba Cloud has released guidance documents such as security white papers and enterprise cloud security guidelines to help users implement secure product deployment.
IVS-06.2: Infrastructure & Virtualization Security - Network Security	*Do you regularly update network architecture diagrams that include data flows between security domains/zones?*	Y			是，阿里云网络团队维护并定期更新网络架构图。	Yes, the Alibaba Cloud network team maintains and regularly updates the network architecture diagram.
IVS-06.3: Infrastructure & Virtualization Security - Network Security	*Do you regularly review for appropriateness the allowed access/connectivity (e.g., firewall rules) between security domains/zones within the network?*	Y			是，阿里云实施监控网络安全状态并进行及时的风险跟进。	Yes, Alibaba Cloud monitors the status of network security and conducts timely risk follow-up.
IVS-06.4: Infrastructure & Virtualization Security - Network Security	*Are all firewall access control lists documented with business justification?*	Y			是，所有的网络访问规则通过平台记录，并且须经过审批后才可进行变更	Yes, all network access rules are recorded by the platform and can only be changed after approval
IVS-07.1: Infrastructure & Virtualization Security - OS Hardening and Base Controls	*Are operating systems hardened to provide only the necessary ports, protocols and services to meet business needs using technical controls (i.e. antivirus, file integrity monitoring and logging) as part of their baseline build standard or template?*	Y			是，阿里云已建立安全基线与加固配置规范，对操作系统与镜像进行加固	Yes, Alibaba Cloud has established a security baseline and hardening configuration requirements to harden the operating system and images
IVS-08.1: Infrastructure & Virtualization Security - Production/Non-Production Environments	*For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?*	Y			是，可由客户自行对其生产环境和非生产环境进行区分。	Yes, customers can devide their production and non-production environments according to their choice.
IVS-08.2: Infrastructure & Virtualization Security - Production/Non-Production Environments	*For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?*	Y			是，阿里云提供了最佳实践和企业上云指引，详见阿里云官网。	Yes, Alibaba Cloud provides best practices and guidelines for enterprises to go to the cloud. For details, see Alibaba Cloud's official website.
IVS-08.3: Infrastructure & Virtualization Security - Production/Non-Production Environments	*Do you logically and physically segregate production and non-production environments?*	Y			是，阿里云对生产环境和非生产环境进行了隔离。	Yes, Alibaba Cloud has isolated production and non-production environments.
IVS-09.1: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure business and customer security requirements?*	Y			是，阿里云依循相关国际标准（如ISO27001/CSA-STAR/PCI-DSS等）建立网络管理机制，且定期由三方审核确认适切性	Yes, Alibaba Cloud establishes a network management mechanism in accordance with relevant international standards (such as ISO27001/CSA-STAR/PCI-DSS, etc.), and regular review by third-party to confirm suitability
IVS-09.2: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure compliance with legislative, regulatory and contractual requirements?*	Y			是，阿里云依循相关国际标准（如ISO27001/CSA-STAR/PCI-DSS等）建立网络管理机制，且定期由三方审核确认适切性	Yes, Alibaba Cloud establishes a network management mechanism in accordance with relevant international standards (such as ISO27001/CSA-STAR/PCI-DSS, etc.), and regular review by third-party to confirm suitability
IVS-09.3: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure separation of production and non-production environments?*	Y			是，阿里云依循相关国际标准（如ISO27001/CSA-STAR/PCI-DSS等）建立网络管理机制，且定期由三方审核确认适切性	Yes, Alibaba Cloud establishes a network management mechanism in accordance with relevant international standards (such as ISO27001/CSA-STAR/PCI-DSS, etc.), and regular review by third-party to confirm suitability
IVS-09.4: Infrastructure & Virtualization Security - Segmentation	*Are system and network environments protected by a firewall or virtual firewall to ensure protection and isolation of sensitive data?*	Y			是，阿里云依循相关国际标准（如ISO27001/CSA-STAR/PCI-DSS等）建立网络管理机制，且定期由三方审核确认适切性	Yes, Alibaba Cloud establishes a network management mechanism in accordance with relevant international standards (such as ISO27001/CSA-STAR/PCI-DSS, etc.), and regular review by third-party to confirm suitability

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IVS-10.1: Infrastructure & Virtualization Security - VM Security	*Are secured and encrypted communication channels used when migrating physical servers, applications or data to virtual servers?*	Y			是，阿里云的数据传输安全是通过数据传输链路加密来保障的。传输加密是指云产品为用户访问（包括读取和上传）数据提供了SSL/TLS协议来保证数据传输的安全。例如，用户如果通过阿里云控制台操作，阿里云控制台会使用HTTPS进行数据传输。所有的阿里云产品都为客户提供了支持HTTPS的API访问点，并提供高达256位密钥的传输加密强度，满足敏感数据加密传输需求。	Yes, Alibaba Cloud's data transmission security is guaranteed by data transmission link encryption. Transmission encryption means that cloud products provide SSL/TLS protocol for users to access (including read and upload) data to ensure the security of data transmission. For example, if the user operates through the Alibaba Cloud console, the Alibaba Cloud console will use HTTPS for data transmission. All Alibaba Cloud products provide customers with API access points that support HTTPS, and provide transmission encryption strength of up to 256-bit keys to meet sensitive data encryption transmission requirements.
IVS-10.2: Infrastructure & Virtualization Security - VM Security	*Do you use a network segregated from production-level networks when migrating physical servers, applications or data to virtual servers?*	Y			是，阿里云的生产网与非生产网隔离。	Yes, Alibaba Cloud's production network is isolated from non-production networks.
IVS-11.1: Infrastructure & Virtualization Security - Hypervisor Hardening	*Do you restrict personnel access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems based on 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)?*	Y			是，阿里云严格管控生产系统的访问权限，所有的访问均有日志记录并纳入入侵检测和日志审计的范畴。	Yes, Alibaba Cloud strictly controls the access rights of the production system. All accesses are logged and included in the scope of intrusion detection and log audit.
IVS-12.1: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms configured and implemented to protect the wireless network environment perimeter and to restrict unauthorized wireless traffic?*	Y			是，阿里云建立了严格的无线网络管控机制，以防止对生产网的非授权访问。	Yes, Alibaba Cloud has established a strict wireless network management and control mechanism to prevent unauthorized access to the production network.
IVS-12.2: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms implemented to ensure wireless security settings are enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings)*	Y			是，阿里云对使用的无线网络均进行了安全配置加固，以防止非授权人员的对相关资源的访问。	Yes, Alibaba Cloud has strengthened the security configuration of the wireless networks used to prevent unauthorized persons from accessing related resources.
IVS-12.3: Infrastructure & Virtualization Security - Wireless Security	*Are policies and procedures established and mechanisms implemented to protect wireless network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?*	Y			是，阿里云建立了网络入侵防护体系，通过工具实时/准实时探测非授权访问。	Yes, Alibaba Cloud has established a network intrusion prevention system that detects unauthorized access in real-time/near-real-time through tools.
IVS-13.1: Infrastructure & Virtualization Security - Network Architecture	*Do your network architecture diagrams clearly identify high-risk environments and data flows that may have legal compliance impacts?*	Y			是，阿里云维护并更新网络架构图，并实时分析评估相关法律合规风险。	Yes, Alibaba Cloud maintains and updates the network architecture diagram, and analyzes and evaluates relevant legal compliance risks in real time.
IVS-13.2: Infrastructure & Virtualization Security - Network Architecture	*Do you implement technical measures and 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?*	Y			是，阿里云的安全监控主要分为日志收集、异常分析检测和告警展示三个部分。日志收集主要是将平台侧的主机日志、网络日志、应用层和云产品的日志进行收集，并分别导入实时计算平台和离线计算平台。异常分析检测会在各个计算平台中，通过安全监控算法模型，对日志进行处理和分析，进而完成风险的发现与监控。一旦发现异常安全事件，会在阿里云内部的安全监控平台上进行告警展示，并通过钉钉，短信，邮件通知等方式通知安全应急人员在第一时间进行响应处置。	Yes, Alibaba Cloud's security monitoring is mainly divided into three parts: log collection, anomaly analysis and detection, and alarm display. Log collection is mainly to collect host logs, network logs, application layer and cloud product logs on the platform side and import them to the real-time computing platform and offline computing platform, respectively. Anomaly analysis and detection will process and analyze logs through security monitoring algorithm models in various computing platforms to complete risk discovery and monitoring. Once abnormal security events are found, alarms will be displayed on Alibaba Cloud's internal security monitoring platform, and security emergency personnel will be notified by nailing, text messaging, email notification, etc. to respond and deal with them as soon as possible.

Interoperability and Portability: Controls IPY-01 through IPY-05

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IPY-01.1: Interoperability & Portability - APIs	*Do you publish a list of all APIs available in the service and indicate which are standard and which are customized?*	Y			是，阿里云已有发布API相关的操作信息，详情请参阅阿里云官网文档	Yes, Alibaba Cloud has released API-related operation information. For details, please refer to the Alibaba Cloud official website documentation.
IPY-02.1: Interoperability & Portability - Data Request	*Is unstructured customer data available on request in an industry-standard format (e.g., .doc, .xls, or .pdf)?*	Y			是，阿里云已有发布API相关的操作信息，详情请参阅阿里云官网文档	Yes, Alibaba Cloud has released API-related operation information. For details, please refer to the Alibaba Cloud official website documentation.
IPY-03.1: Interoperability & Portability - Policy & Legal	*Do you provide policies and procedures (i.e. service level agreements) governing the use of APIs for interoperability between your service and third- party applications?*	Y			是，阿里云已有发布API相关的操作信息，详情请参阅阿里云官网文档	Yes, Alibaba Cloud has released API-related operation information. For details, please refer to the Alibaba Cloud official website documentation.
IPY-03.2: Interoperability & Portability - Policy & Legal	*Do you provide policies and procedures (i.e. service level agreements) governing the migration of application data to and from your service?*	Y			是，阿里云各产品有制定相应的服务水平协议，说明客户数据的保管责任认信	Yes, each product of Alibaba Cloud has a corresponding service level agreement, stating the responsibility of customer data storage
IPY-04.1: Interoperability & Portability - Standardized Network Protocols	*Can data import, data export and service management be conducted over secure (e.g., non-clear text and authenticated), industry accepted standardized network protocols?*	Y			是，数据传输的过程中可使用行业通用的网络传输加密协定	Yes, the industry-wide network transmission encryption protocol can be used during data transmission
IPY-04.2: Interoperability & Portability - Standardized Network Protocols	*Do you provide consumers (tenants) with documentation detailing the relevant interoperability and portability network protocol standards that are involved?*	Y			是，数据传输的过程中可使用行业通用的网络传输加密协定	Yes, the industry-wide network transmission encryption protocol can be used during data transmission

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
IPY-05.1: Interoperability & Portability - Virtualization	*Do you use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability?*	Y			是，阿里云的镜像导出与导入采用行业通用的OVF及其他格式	Yes, Alibaba Cloud's image export and import uses the industry's common OVF and other formats
IPY-05.2: Interoperability & Portability - Virtualization	*Do you have documented custom changes made to any hypervisor in use, and all solution-specific virtualization hooks available for customer review?*	Y			是，阿里云已有留存相关记录。	Yes, Alibaba Cloud has retained relevant records.
Mobile Security: Controls MOS-01 through MOS-20						
MOS-01.1: Mobile Security - Anti-	*Do you provide anti-malware training specific to mobile devices as part of your information security awareness training?*	Y			是，阿里云提供的新员工培训和全员年度的安全培训中，都包含了恶意代码防范的意识和技能。	Yes, the new employee training and annual security training provided by Alibaba Cloud both include awareness and skills in malicious code prevention.
MOS-02.1: Mobile Security - Application Stores	*Do you document and make available lists of approved application stores for mobile devices accessing or storing company data and/or company systems?*	Y			是，阿里云提供了统一的平台供员工下载办公软件。	Yes, Alibaba Cloud provides a unified platform for employees to download office software.
MOS-03.1: Mobile Security - Approved Applications	*Do you have a policy enforcement capability (e.g., XACML) to ensure that only approved applications and those from approved application stores be loaded onto a mobile device?*	Y			是，阿里云利用自动化工具扫描员工的移动办公终端，以发现是否安装了非授权软件在移动终端上。	Yes, Alibaba Cloud uses automated tools to scan employees' mobile office terminals to find out if unauthorized software is installed on the mobile terminals.
MOS-04.1: Mobile Security - Approved Software for BYOD	*Does your BYOD policy and training clearly state which applications and applications stores are approved for use on BYOD devices?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment.
MOS-05.1: Mobile Security - Awareness and Training	*Do you have a documented mobile device policy in your employee training that clearly defines mobile devices and the accepted usage and requirements for mobile devices?*	Y			是，阿里云遵循的安全红线中明确了对移动设备的安全要求，同时这些要求也都在每年的安全培训中进行全员宣导。	Yes, the security red line followed by Alibaba Cloud clearly specifies the security requirements for mobile devices. At the same time, these requirements are all publicized during the annual security training.
MOS-06.1: Mobile Security - Cloud Based Services	*Do you have a documented list of pre-approved cloud based services that are allowed to be used for use and storage of company business data via a mobile device?*	Y			是，阿里云仅允许员工使用公司自研发的云存储产品/服务。	Yes, Alibaba Cloud only allows employees to use the company's self-developed cloud storage products/services.
MOS-07.1: Mobile Security -	*Do you have a documented application validation process for testing device, operating system and application compatibility issues?*	Y			是，软件的兼容性是阿里云对软件的基本要求中的关注点。	Yes, software compatibility is the focus of Alibaba Cloud's basic software requirements.
MOS-08.1: Mobile Security - Device Eligibility	*Do you have a BYOD policy that defines the device(s) and eligibility requirements allowed for BYOD usage?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment.
MOS-09.1: Mobile Security - Device Inventory	*Do you maintain an inventory of all mobile devices storing and accessing company data which includes device status (os system and patch levels, lost or decommissioned, device assignee)?*	Y			是，阿里云所有的移动办公设备均需要在公司的终端管理系统上进行注册。	Yes, all Alibaba Cloud mobile office equipment needs to be registered on the company's terminal management system.
MOS-10.1: Mobile Security - Device Management	*Do you have a centralized mobile device management solution deployed to all mobile devices that are permitted to store, transmit, or process company data?*	Y			是，阿里云有集中的终端管理系统进行移动办公设备的统一管理。	Yes, Alibaba Cloud has a centralized terminal management system for unified management of remote working equipment.
MOS-11.1: Mobile Security - Encryption	*Does your mobile device policy require the use of encryption for either the entire device or for data identified as sensitive enforceable through technology controls for all mobile devices?*	Y			是，阿里云的移动设备安全策略明确要求对接触敏感数据的移动设备进行硬盘加密。	Yes, Alibaba Cloud 's mobile device security policy explicitly requires hard drive encryption for mobile devices that come into contact with sensitive data.
MOS-12.1: Mobile Security - Jailbreaking and Rooting	*Does your mobile device policy prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting)?*	Y			是，阿里云的移动设备安全策略禁止对公司派发的移动设备绕过内置的安全管控（如越狱），并通过终端管理软件进行监控。	Yes, Alibaba Cloud 's mobile device security policy prohibits mobile devices distributed by the company from bypassing built-in security controls (such as jailbreak) and monitoring through terminal management software.
MOS-12.2: Mobile Security - Jailbreaking and Rooting	*Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?*	Y			是，阿里云的移动设备安全策略禁止对公司派发的移动设备绕过内置的安全管控（如越狱），并通过终端管理软件进行监控。	Yes, Alibaba Cloud 's mobile device security policy prohibits mobile devices distributed by the company from bypassing built-in security controls (such as jailbreak) and monitoring through terminal management software.
MOS-13.1: Mobile Security - Legal	*Does your BYOD policy clearly define the expectation of privacy, requirements for litigation, e- discovery and legal holds?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment.
MOS-13.2: Mobile Security - Legal	*Do you have detective and preventative controls on the device or via a centralized device management system which prohibit the circumvention of built-in security controls?*	Y			是，阿里云有统一的终端管理系统进行移动设备管理。	Yes, Alibaba Cloud has a unified terminal management system for mobile device management.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
MOS-14: Mobile Security - Lockout Screen	*Do you require and enforce via technical controls an automatic lockout screen for BYOD and company owned devices?*	Y			是，通过技术实现对锁屏策略的设置。	Yes, setting the lock screen strategy through technology.
MOS-15: Mobile Security - Operating Systems	*Do you manage all changes to mobile device operating systems, patch levels and applications via your company's change management processes?*	Y			是，所有对操作系统的补丁升级变更都会被监控。	Yes, all patch updates to the operating system are monitored.
MOS-16.1: Mobile Security - Passwords	*Do you have password policies for enterprise issued mobile devices and/or BYOD mobile devices?*	Y			是，阿里云通过系统配置了密码安全策略。	Yes, Alibaba Cloud has configured a password security policy through the system.
MOS-16.2: Mobile Security - Passwords	*Are your password policies enforced through technical controls (i.e. MDM)?*	Y			是，阿里云系统化实现密码的安全策略配置。	Yes, Alibaba Cloud systematically implements password security policy configuration.
MOS-16.3: Mobile Security - Passwords	*Do your password policies prohibit the changing of authentication requirements (i.e. password/PIN length) via a mobile device?*	Y			是，阿里云的密码安全策略里面有认证的相关配置要求，如密码长度。	Yes, Alibaba Cloud's password security policy has authentication-related configuration requirements, such as password length.
MOS-17.1: Mobile Security - Policy	*Do you have a policy that requires BYOD users to perform backups of specified corporate data?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。同时，禁止办公数据在BYOD的设备上进行本地存储。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment. At the same time, local storage of office data on BYOD devices is prohibited.
MOS-17.2: Mobile Security - Policy	*Do you have a policy that requires BYOD users to prohibit the usage of unapproved application stores?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。同时，禁止办公数据在BYOD的设备上进行本地存储。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment. At the same time, local storage of office data on BYOD devices is prohibited.
MOS-17.3: Mobile Security - Policy	*Do you have a policy that requires BYOD users to use anti-malware software (where supported)?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。同时，禁止办公数据在BYOD的设备上进行本地存储。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment. At the same time, local storage of office data on BYOD devices is prohibited.
MOS-18.1: Mobile Security - Remote Wipe	*Does your IT provide remote wipe or corporate data wipe for all company-accepted BYOD devices?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。同时，禁止办公数据在BYOD的设备上进行本地存储。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment. At the same time, local storage of office data on BYOD devices is prohibited.
MOS-18.2: Mobile Security - Remote Wipe	*Does your IT provide remote wipe or corporate data wipe for all company-assigned mobile devices?*	Y			是，阿里云针对接触敏感数据的设备提供远程清除设备数据的能力。	Yes, Alibaba Cloud provides the ability to remotely erase device data for devices exposed to sensitive data.
MOS-19.1: Mobile Security - Security Patches	*Do your mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier?*	Y			是，阿里云通过终端安全软件统一管理以保证设备上安全补丁及时更新。	Yes, Alibaba Cloud uses unified management of terminal security software to ensure that security patches on devices are updated in a timely manner.
MOS-19.2: Mobile Security - Security Patches	*Do your mobile devices allow for remote validation to download the latest security patches by company IT personnel?*	Y			是，阿里云允许移动设备远程下载最新的安全补丁。	Yes, Alibaba Cloud allows mobile devices to remotely download the latest security patches.
MOS-20.1: Mobile Security - Users	*Does your BYOD policy clarify the systems and servers allowed for use or access on the BYOD-enabled device?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。同时，禁止办公数据在BYOD的设备上进行本地存储。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment. At the same time, local storage of office data on BYOD devices is prohibited.
MOS-20.2: Mobile Security - Users	*Does your BYOD policy specify the user roles that are allowed access via a BYOD-enabled device?*	Y			是，阿里云禁止对办公电脑BYOD，其他设备如需BYOD(如手机）则需要在终端管理系统进行注册绑定员工身份，且只可访问办公网络环境。同时，禁止办公数据在BYOD的设备上进行本地存储。	Yes, Alibaba Cloud prohibits BYOD for office computers. For other devices that require BYOD (such as mobile phones), they need to register with the terminal management system to bind employees, and they can only access the office network environment. At the same time, local storage of office data on BYOD devices is prohibited.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
Security Incident Management, E-Discovery & Cloud Forensics: Controls SEF-01 through SEF-05						
SEF-01.1: Security Incident Management, E-Discovery & Cloud Forensics - Contact/Authority Maintenance	*Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立安全事件管理流程，包含发现、调查、通报、解决、复盘等流程，包含对客户的沟通与协作机制	Yes, Alibaba Cloud establishes security incident management processes in accordance with relevant international standards (such as ISO27001/27017/27018, etc.), including processes such as discovery, investigation, notification, resolution, and review, including customer communication and collaboration mechanism
SEF-02.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Do you have a documented security incident response plan?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立安全事件管理流程，包含发现、调查、通报、解决、复盘等流程，包含对客户的沟通与协作机制	Yes, Alibaba Cloud establishes security incident management processes in accordance with relevant international standards (such as ISO27001/27017/27018, etc.), including processes such as discovery, investigation, notification, resolution, and review, including customer communication and collaboration mechanism
SEF-02.2: Security Incident Management, E Discovery & Cloud Forensics - Incident Management	*Do you integrate customized tenant requirements into your security incident response plans?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立安全事件管理流程，包含发现、调查、通报、解决、复盘等流程，包含对客户的沟通与协作机制	Yes, Alibaba Cloud establishes security incident management processes in accordance with relevant international standards (such as ISO27001/27017/27018, etc.), including processes such as discovery, investigation, notification, resolution, and review, including customer communication and collaboration mechanism
SEF-02.3: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?*	Y			是，于阿里云的安全白皮书与服务协议内已有说明客户与阿里云的责任义务	Yes, the responsibilities of the customer and Alibaba Cloud have been stated in Alibaba Cloud's security white paper and service agreement.
SEF-02.4: Security Incident Management, E-Discovery & Cloud Forensics - Incident Management	*Have you tested your security incident response plans in the last year?*	Y			是，阿里云每年至少进行一次安全事件应变流程审阅与测试	Yes, Alibaba Cloud reviews and tests security incident response processes at least once a year
SEF-03.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Reporting	*Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?*	Y			是，阿里云通过系统化的方式自动收集相关日志信息，作为后续调查与审计的基础	Yes, Alibaba Cloud automatically collects relevant log information in a systematic manner as the basis for subsequent investigations and audits
SEF-03.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Reporting	*Does your logging and monitoring framework allow isolation of an incident to specific tenants?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立安全事件管理流程，包含发现、调查、通报、解决、复盘等流程，包含对客户的沟通与协作机制	Yes, Alibaba Cloud establishes security incident management processes in accordance with relevant international standards (such as ISO27001/27017/27018, etc.), including processes such as discovery, investigation, notification, resolution, and review, including customer communication and collaboration mechanisms
SEF-04.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes and controls?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立安全事件管理流程，包含发现、调查、通报、解决、复盘等流程，包含对客户的沟通与协作机制	Yes, Alibaba Cloud establishes security incident management processes in accordance with relevant international standards (such as ISO27001/27017/27018, etc.), including processes such as discovery, investigation, notification, resolution, and review, including customer communication and collaboration mechanisms
SEF-04.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立安全事件管理流程，包含发现、调查、通报、解决、复盘等流程，包含对客户的沟通与协作机制	Yes, Alibaba Cloud establishes security incident management processes in accordance with relevant international standards (such as ISO27001/27017/27018, etc.), including processes such as discovery, investigation, notification, resolution, and review, including customer communication and collaboration mechanisms
SEF-04.3: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立安全事件管理流程，包含发现、调查、通报、解决、复盘等流程，包含对客户的沟通与协作机制	Yes, Alibaba Cloud establishes security incident management processes in accordance with relevant international standards (such as ISO27001/27017/27018, etc.), including processes such as discovery, investigation, notification, resolution, and review, including customer communication and collaboration mechanisms

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
SEF-04.4: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Legal Preparation	*Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?*	Y			是，阿里云依循相关国际标准（如ISO27001/27017/27018等）建立安全事件管理流程，包含发现、调查、通报、解决、复盘等流程，包含对客户的沟通与协作机制	Yes, Alibaba Cloud establishes security incident management processes in accordance with relevant international standards (such as ISO27001/27017/27018, etc.), including processes such as discovery, investigation, notification, resolution, and review, including customer communication and collaboration mechanisms
SEF-05.1: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Metrics	*Do you monitor and quantify the types, volumes and impacts on all information security incidents?*	Y			是，当信息安全事件发生时，相应的过程记录会被完整记录及复盘	Yes, when an information security incident occurs, the corresponding process records will be fully recorded and reviewed
SEF-05.2: Security Incident Management, E-Discovery & Cloud Forensics - Incident Response Metrics	*Will you share statistical information for security incident data with your tenants upon request?*	Y			是，当信息安全事件影响客户时，阿里云会及时与客户同步处理进度	Yes, when information security incidents affect customers, Alibaba Cloud will synchronize the progress with customers in a timely manner

Supply Chain Management, Transparency and Accountability: Controls STA- 01 through STA-09

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
STA-01.1: Supply Chain Management, Transparency and Accountability - Data Quality and Integrity	*Do you inspect and account for data quality errors and associated risks, and work with your cloud supply- chain partners to correct them?*	Y			是，阿里云已有制定供应商管理规范，且针对供应商制定了数据安全的管理规范并建立了定期第三方数据安全审计的机制。	Yes, Alibaba Cloud has established supplier management policy, but it is not currently relying on partners to deliver products
STA-01.2: Supply Chain Management, Transparency and Accountability - Data Quality and Integrity	*Do you design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least- privileged access for all personnel within your supply chain?*	Y			是，阿里云已有制定供应商管理规范，且针对供应商制定了数据安全的管理规范并建立了定期第三方数据安全审计的机制。	Not applicable, although Alibaba Cloud has established supplier management policy, but it has not relied on partners to deliver products
STA-02.1: Supply Chain Management, Transparency and Accountability - Incident Reporting	*Do you make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals)?*	Y			是，当信息安全事件影响客户时，阿里云会及时与客户同步处理进度	Yes, when information security incidents affect customers, Alibaba Cloud will synchronize the progress with customers in a timely manner
STA-03.1: Supply Chain Management, Transparency and Accountability - Network/Infrastructure Services	*Do you collect capacity and use data for all relevant components of your cloud service offering?*	Y			是，阿里云通过收集这些信息调校与优化产品的服务能力	Yes, Alibaba Cloud collects this information to adjust and optimize product service capabilities
STA-03.2: Supply Chain Management, Transparency and Accountability - Network/Infrastructure Services	*Do you provide tenants with capacity planning and use reports?*			NA	不适用，客户的使用资源由客户自身管理与规划，与阿里云自身的资源管理无直接关联性	Not applicable, the customer's use of resources is managed and planned by the customer, and has no direct relationship with Alibaba Cloud's own resource management
STA-04.1: Supply Chain Management, Transparency and Accountability - Provider Internal Assessments	*Do you perform annual internal assessments of conformance and effectiveness of your policies, procedures, and supporting measures and metrics?*	Y			是，阿里云依循相关国际标准（如ISO20000）建立服务水平管理流程，至少每年一次审阅服务水平协议内容	Yes, Alibaba Cloud establishes service level management processes in accordance with relevant international standards (such as ISO20000), and reviews the content of the service level agreement at least once a year
STA-05.1: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed, stored and transmitted?*	Y			是，虽阿里云目前没有委外的数据处理者，但已有制定相应协议与管理规范	Yes, although Alibaba Cloud currently does not have outsourced data processors, it has formulated corresponding protocols and management policies.
STA-05.2: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?*	Y			是，虽阿里云目前没有委外的数据处理者，但已有制定相应协议与管理规范	Yes, although Alibaba Cloud currently does not have outsourced data processors, it has formulated corresponding agreements and management policies.

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
STA-05.3: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Does legal counsel review all third- party agreements?*	Y			是，阿里云的所有协议皆由法务团队审阅与确认	Yes, all Alibaba Cloud agreements are reviewed and checked by the legal team
STA-05.4: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do third-party agreements include provision for the security and protection of information and assets?*	Y			是，阿里云在供应商管理流程内已纳入安全与隐私相关的要求，且在双方的合同内纳入相应管理要求，确保供应商必须遵循相关的要求	Yes, Alibaba Cloud has included security and privacy related requirements in the supplier management process, and included the corresponding management requirements in the contract between the two parties to ensure that the supplier must comply with the relevant requirements
STA-05.5: Supply Chain Management, Transparency and Accountability - Supply Chain Agreements	*Do you provide the client with a list and copies of all sub-processing agreements and keep this updated?*			NA	不适用，阿里云目前没有委外的数据处理者	No applicable, Alibaba Cloud currently has no outsourced data processors
STA-06.1: Supply Chain Management, Transparency and Accountability - Supply Chain Governance Reviews	*Do you review the risk management and governance processes of partners to account for risks inherited from other members of that partner's supply chain?*	Y			是，阿里云的合同模板内已有纳入安全与隐私相关要求，并且说明对于供应商的检查与审计需求，确保供应商的服务能力	Yes, Alibaba Cloud's contract template has included security and privacy related requirements, and explained the inspection and audit requirements for suppliers to ensure supplier service capabilities
STA-07.1: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Are policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g., SLAs) between providers and customers (tenants)?*	Y			是，阿里云的合同模板内已有纳入安全与隐私相关要求，并且说明对于供应商的检查与审计需求，确保供应商的服务能力	Yes, Alibaba Cloud's contract template has included security and privacy related requirements, and explained the inspection and audit requirements for suppliers to ensure supplier service capabilities
STA-07.2: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Do you have the ability to measure and address non- conformance of provisions and/or terms across the entire supply chain (upstream/downstr eam)?*	Y			是，阿里云的合同模板内已有纳入安全与隐私相关要求，并且说明对于供应商的检查与审计需求，确保供应商的服务能力	Yes, Alibaba Cloud's contract template has included security and privacy related requirements, and explained the inspection and audit requirements for suppliers to ensure supplier service capabilities
STA-07.3: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Can you manage service-level conflicts or inconsistencies resulting from disparate supplier relationships?*	Y			是，阿里云的合同模板内已有纳入安全与隐私相关要求，并且说明对于供应商的检查与审计需求，确保供应商的服务能力	Yes, Alibaba Cloud's contract template has included security and privacy related requirements, and explained the inspection and audit requirements for suppliers to ensure supplier service capabilities
STA-07.4: Supply Chain Management, Transparency and Accountability - Supply Chain Metrics	*Do you review all agreements, policies and processes at least annually?*	Y			是，阿里云的合同模板内已有纳入安全与隐私相关要求，并且说明对于供应商的检查与审计需求，确保供应商的服务能力	Yes, Alibaba Cloud's contract template has included security and privacy related requirements, and explained the inspection and audit requirements for suppliers to ensure supplier service capabilities
STA-08.1: Supply Chain Management, Transparency and Accountability - Third Party Assessment	*Do you assure reasonable information security across your information supply chain by performing an annual review?*	Y			是，阿里云的合同模板内已有纳入安全与隐私相关要求，并且说明对于供应商的检查与审计需求，确保供应商的服务能力	Yes, Alibaba Cloud's contract template has included security and privacy related requirements, and explained the inspection and audit requirements for suppliers to ensure supplier service capabilities
STA-08.2: Supply Chain Management, Transparency and Accountability - Third Party Assessment	*Does your annual review include all partners/third- party providers upon which your information supply chain depends?*	Y			是，阿里云的合同模板内已有纳入安全与隐私相关要求，并且说明对于供应商的检查与审计需求，确保供应商的服务能力	Yes, Alibaba Cloud's contract template has included security and privacy related requirements, and explained the inspection and audit requirements for suppliers to ensure supplier service capabilities
STA-09.1: Supply Chain Management, Transparency and Accountability - Third Party Audits	*Do you permit tenants to perform independent vulnerability assessments?*	Y			是，客户可对自己的资源进行漏洞扫描评估	Yes, customers can conduct vulnerability scan assessments of their own resources
STA-09.2: Supply Chain Management, Transparency and Accountability - Third Party Audits	*Do you have external third party services conduct vulnerability scans and periodic penetration tests on your applications and networks?*	Y			是，阿里云至少每半年要求三方进行一次外部渗透测试	Yes, Alibaba Cloud requires third-party to conduct external penetration testing at least once every six months

Control ID in CCM	Consensus Assessment Questions	Yes	No	N/A	Notes in Chinese	Notes in English
Threat and Vulnerability Management: Controls TVM-01 through TVM-03						
TVM-01.1: Threat and Vulnerability Management - Anti-Virus/Malicious Software	*Do you have anti- malware programs that support or connect to your cloud service offerings installed on all of your systems?*	Y			是，阿里云在云平台侧建立了恶意软件防护机制，并在云安全中心提供恶意软件防护能力供客户使用。	Yes, Alibaba Cloud has established a malware protection mechanism on the cloud platform side, and provided malware protection capabilities in the Cloud Security Center for customers to use.
TVM-01.2: Threat and Vulnerability Management - Anti-Virus/Malicious Software	*Do you ensure that security threat detection systems using signatures, lists or behavioral patterns are updated across all infrastructure components within industry accepted time frames?*	Y			是，阿里云的入侵检测防护系统持续更新，以保证对外部威胁的监测发现。	Yes, Alibaba Cloud's intrusion detection and protection system is continuously updated to ensure the detection and detection of external threats.
TVM-02.1: Threat and Vulnerability Management - Vulnerability/Patch Management	*Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			是，阿里云定期执行网络、系统及应用层的漏洞扫描，漏洞扫描的工具遵循行业最佳实践。	Yes, Alibaba Cloud regularly performs vulnerability scans at the network, system, and application layers. The tools for vulnerability scans follow industry best practices.
TVM-02.2: Threat and Vulnerability Management - Vulnerability/Patch Management	*Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			是，阿里云定期执行网络、系统及应用层的漏洞扫描，漏洞扫描的工具遵循行业最佳实践。	Yes, Alibaba Cloud regularly performs vulnerability scans at the network, system, and application layers. The tools for vulnerability scans follow industry best practices.
TVM-02.3: Threat and Vulnerability Management - Vulnerability/Patch Management	*Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?*	Y			是，阿里云定期执行网络、系统及应用层的漏洞扫描，漏洞扫描的工具遵循行业最佳实践。	Yes, Alibaba Cloud regularly performs vulnerability scans at the network, system, and application layers. The tools for vulnerability scans follow industry best practices.
TVM-02.4: Threat and Vulnerability Management - Vulnerability/Patch Management	*Will you make the results of vulnerability scans available to tenants at their request?*		N		否，阿里云目前尚未将扫描结果提供给客户。	No, Alibaba Cloud doesn't provide the scan results to customers.
TVM-02.5: Threat and Vulnerability Management - Vulnerability/Patch Management	*Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications and systems?*	Y			是，阿里云依循相关国际标准（如ISO20000/27001/CSA-STAR/PCI-DSS等）建立变更管理规范，漏洞补丁包可经过变更流程部署至相应的环境内	Yes, Alibaba Cloud establishes change management policy in accordance with relevant international standards (such as ISO20000/27001/CSA-STAR/PCI-DSS, etc.). Vulnerability patch packages can be deployed to the corresponding environment through the change process
TVM-02.6: Threat and Vulnerability Management - Vulnerability/Patch Management	*Will you provide your risk-based systems patching time frames to your tenants upon request?*		N		否，对外仅发送漏洞通告，但阿里云内部已有规范漏洞修补机制，包含定级与相应的修复时限，修补的通知会同步发布于官网	No, only vulnerability notifications are sent to the outside, but Alibaba Cloud already has a standard vulnerability patching mechanism, including rating and corresponding repair deadlines. Patched notifications will be posted on the official website simultaneously.
TVM-03.1: Threat and Vulnerability Management - Mobile Code	*Is mobile code authorized before its installation and use, and the code configuration checked, to ensure that the authorized mobile code operates according to a clearly defined security policy?*			NA	不适用，阿里云平台未使用移动代码	Not applicable, Alibaba Cloud platform does not rely on mobile code
TVM-03.2: Threat and Vulnerability Management - Mobile Code	*Is all unauthorized mobile code prevented from executing?*			NA	不适用，阿里云平台未使用移动代码	Not applicable, Alibaba Cloud platform does not rely on mobile code