系统和组织控制 3（SOC3）报告

阿里云的云服务系统

安全性、可用性和

保密性报告

报告期间：2018 年 11 月 1 日至 2019 年 12 月 31 日

本报告以英文版形式出具，中文翻译版仅作为参考，如有任何差异，以英文版报告为准

独立服务审计师报告

致阿里云计算有限公司管理层：

范围

我们检查了阿里云后附的“阿里云管理层关于云服务系统的认定”（“该认定”），即阿里云云服务系统（“系统”）的控制在 2018 年 11 月 1 日至 2019 年 12 月 31 日期间有效，以根据 TSP 第 100 条“针对安全性、可用性、过程完整性、保密性和隐私性的 2017 版信托服务标准(AICPA，信托服务标准)”中所列示的与安全性、可用性、保密性相关的信托服务标准(“适用信托服务标准”)，为实现阿里云的服务承诺和系统需求提供合理保证的控制的设计适当性和运行有效性。

服务机构的责任

阿里云负责其服务承诺和系统需求，并在相关体系中设计、实施并运行有效控制，以为实现阿里云的服务承诺和系统需求提供合理保证。阿里云还提供了关于系统控制有效性的认定。在编制其认定时，阿里云负责选择和识别在其认定中适用的信托服务标准，并通过评估系统的控制有效性来为其认定提供合理依据。

服务审计师的职责

我们的责任是基于我们的检查，就管理层关于系统控制在整个审计期间内的有效性的认定发表意见，以合理保证服务机构根据适用的信托服务标准实现其服务承诺并满足系统需求我们根据美国注册会计师协会颁布的鉴证准则执行本检查。这些准则要求我们在计划和执行审查时，就在所有重大方面，就管理层的认定是否公正，获取合理保证。我们认为，我们获取的证据是充分和适当的，为发表意见提供了合理基础。

我们的检查包括：

- 了解体系及服务机构的服务承诺和系统需求
- 评估控制无法根据适用的信托服务标准有效实现阿里云的服务承诺并满足系统需求的风险
- 实施相关程序以获取证据，表明系统的控制是否根据适用的信托服务标准有效实现阿里云的服务承诺并满足系统需求

我们的检查还包括在适当情况下实施我们认为必要的其他程序。

固有限制

内部控制的任何体系的有效性都存在固有限制，包括可能存在的人为失误及控制规避等。

由于其性质，控制并非总能根据适用的信托服务标准为实现服务机构的服务承诺和系统需求有效运行。根据控制设计适当性和运行有效性的任何结论来推断未来期间的状况，将面临控制因为条件变化或遵守政策或程序的程度减轻而可能变得不够充分的风险。

意见

我们认为，在所有重大方面，管理层关于阿里云云服务系统的控制认定在 2018 年 11 月 1 日至 2019 年 12 月 31 日期间有效，为以下陈述提供合理保证：阿里云根据适用的信托服务标准实现其服务承诺并满足系统需要的声明是公正的。

罗兵咸永道会计师事务所

中国香港

2020 年 2 月 14 日

Alibaba Cloud

2018 年 11 月 1 日至 2019 年 12 月 31 日期间阿里云管理层关于云服务系统的认定

我们负责设计、实施、运行和维护阿里云计算有限公司及其附属公司（包括但不限于阿里云（新加坡）私人有限公司、阿里巴巴（欧洲）有限公司以及阿里云美国有限责任公司、阿里云（印度）有限责任公司、阿里云（马来西亚）私人有限公司，阿里云计算有限公司及其附属公司统称为“服务组织”或“阿里云”）在 2018 年 11 月 1 日至 2019 年 12 月 31 日期间的云服务系统（“系统”）相关的有效控制，就阿里云实现其安全性、可用性和保密性相关的服务承诺和满足系统需求提供合理保证。我们后附的体系说明确定认定涵盖系统的各个方面。

我们已对 2018 年 11 月 1 日至 2019 年 12 月 31 日期间体系控制的有效性执行了评估，以根据 TSP 第 100 条“针对安全性、可用性、过程完整性、保密性和隐私性的 2017 版信托服务标准(AICPA，信托服务标准)”中所列示的与安全性、可用性、保密性相关的信托服务标准(“适用信托服务标准”)，就阿里云实现其服务承诺并满足系统需求提供合理保证。阿里云体系应用适用的信托服务标准的目标体现在与适用的信托服务标准相关的服务承诺和系统需求中。与适用的信托服务标准相关的主要服务承诺和系统需求如下：

- 保护体系免受未授权访问、使用或修改，以满足实体的承诺和系统需求；。
- 指定的保密信息按承诺或协议受体系保护；以及
- 可按承诺或协议运行和使用体系。

任何内部控制都存在固有限制，包括人为错误以及规避管控的可能性。受这些固有限制影响，服务机构可能就实现其服务承诺并满足系统需求获得合理（但不是绝对）保证。

我们声明，体系控制在 2018 年 11 月 1 日至 2019 年 12 月 31 日期间有效，以合理保证阿里云根据适用的信托服务标准实现其服务承诺并满足系统需求。

阿里云计算有限公司

2020 年 2 月 14 日

2018 年 11 月 1 日至 2019 年 12 月 31 日期间阿里云的云服务系统说明

I. 概述

业务描述

阿里云是阿里巴巴集团（纽交所股票代码：BABA，简称“阿里巴巴”或“集团”）旗下公司，为我们的全球客户和合作伙伴以及阿里云自有电子商务生态系统提供一整套全面的全球云计算服务。阿里云提供的云服务由自主开发的云服务平台和技术提供支持。阿里云旨在通过大力投资技术创新，不断提高其服务的计算能力和规模经济，将云计算转变为最先进的计算基础设施。云服务已广泛应用于各个行业，包括金融、政府、游戏、电子商务、移动服务、医疗服务和多媒体等。除云服务外，阿里云还为智能生活、智慧城市、智能制造和智慧农业等广泛领域提供物联网平台。阿里云致力于打造物联网基础设施。阿里云物联网平台的用户十分看重物联网平台的数据存储和处理能力，他们希望与 API 和其他阿里云服务集成，以获得一整套全面的服务。物联网平台具有用于快速数据采集、存储和应用程序开发的规则引擎。阿里云致力于建立覆盖整个行业的集成式云端和设备终端开发平台，搭建一整条物联网产业链，建立全球适用的物联网标准，持续建设物联网生态系统、平台和基础设施，加速物理世界和数字世界的融合，并推动物联网向智联网 (IoI) 的发展。

本报告所涵盖的云服务

阿里云致力于打造一个安全开放的公共云计算服务平台。本报告涵盖以下服务：

1. 云服务器 (ECS)
2. Kubernetes 容器服务
3. 容器镜像服务
4. 对象存储服务 (OSS)
5. 阿里云 CDN (CDN)
6. 网络附加存储 (NAS)
7. 虚拟专有云 (VPC)
8. 高速通道
9. NAT 网关
10. 负载均衡器 (SLB)
11. 弹性 IP
12. VPN 网关
13. 云数据库 MySQL 版
14. 云数据库 SQL Server 版
15. 云数据库 PostgreSQL 版
16. 云数据库 PPAS 版
17. 云数据库 POLARDB 版
18. DDoS 基础防护
19. DDoS 高防

20. DDoS 高防（国际）
21. Web 应用防火墙 (WAF)
22. 安全中心
23. 资源访问控制 (RAM)
24. 密钥管理服务 (KMS)
25. 操作审计
26. 大数据计算服务
27. 日志服务
28. 物联网平台

本报告所涉数据中心位置

阿里云致力于提供稳定、可靠的计算和数据处理能力，进而实现互联世界。阿里云拥有 61 个可用区，遍布全球从西到东 20 个区域。

本报告所涉数据中心位置范围覆盖中国大陆（青岛、北京、张家口、呼和浩特、杭州、上海、深圳和成都）、中国香港、新加坡（新加坡）、印度（孟买）、印度尼西亚（雅加达）、德国（法兰克福）、日本（东京）、澳大利亚（悉尼）、英国（伦敦）、美国（硅谷、弗吉尼亚）、马来西亚（吉隆坡）和阿拉伯联合酋长国（迪拜）。

数据中心和分包服务机构的功能

阿里云通过多个分包服务机构（“分包服务机构”）为数据中心提供暖通空调 (HVAC)。阿里云要求上述分包服务机构通过实施访问控制和环境保障措施（例如灭火器或闭路电视 (CCTV)）来确保场所安全。此外，阿里云要求所有分包服务机构在信息安全和业务连续性方面遵循特定要求。

阿里云负责评估上述分包服务机构的能力和绩效。阿里云与分包服务机构通过订立合约来明确双方的责任和义务，并指定数据中心的服务范围和服务可用性等级。为维持高服务质量，分包服务机构提交一次服务水平协议（“SLA”）报告，阿里云会根据该报告进行绩效评估。上述分包服务机构应提交月度 SLA 报告，并在报告中包含重大事件、各项指标和维护摘要。阿里云会对数据中心提供商的服务水平进行评估，并发布季度评估报告，以确保分包服务机构能够适当地满足阿里云的所有要求。

必须借助合理设计且有效运行的补充子服务组织控制以及阿里云的现有控制，才能根据适用的信任服务标准实现阿里云服务承诺并满足系统要求。本报告的用户应承认，服务审计师的审查并未延伸到子服务组织的实际控制。

II. 主要服务承诺和系统要求

阿里云致力于为客户提供稳定、可靠、安全、合规的云计算服务，帮助客户确保其系统和数据的安全性、保密性和可用性。阿里云负责设计、实施和运行系统和服务相关的有效控制，并就阿里云实现其服务承诺并满足系统要求提供合理保证。对阿里云客户（用户实体）做出的服务承诺将以在线产品服务水平协议（“产品 SLA”）、会员协议、隐私政策、阿里云服务在线说明和合同的形式进行传达。有关产品 SLA、会员协议和其他法律文件的详细信息可在阿里云法律文件中心获取。阿里云还建立了各种客户支持沟通渠道，包括但不限于即时聊天、工单、电子邮件和建议帖等。全球客户支持团队还将通过已建立的各项机制，就任何可能对客户造成影响的潜在问题与客户进行沟通。此外，阿里云还遵循国际标准和最佳实践。与安全性和合规性有关的详细信息均通过安全和合规中心传达给客户。

基于阿里云构建的应用程序的安全性由阿里云和用户实体共同负责。阿里云负责确保底层云服务平台的安全性，并为客户提供安全服务和相关功能，而客户则负责确保基于阿里云服务构建的应用程序的安全性。阿里云的客户应在选择服务和设计云端架构时评估自身目标，同时考虑阿里云的现有控制及其自身在履行安全职责方面应保障的各项配置和运行控制。在设计和提供服务时，为履行对客户的服务承诺并遵守相关法律法规要求，阿里云制定了规定各项系统和操作要求的政策、标准、手册和程序，并在组织范围内广泛沟通。

III. 控制环境、信息和沟通、风险评估、控制活动和监控活动概述

内部控制由阿里云董事会、管理人员和行政人员负责制定和维护。阿里云内部控制由美国注册会计师协会定义的以下五个要素组成：

- **控制环境**——实施内部控制、提供标准要求和体系结构、影响员工内部控制意识的基础；
- **信息和沟通**——确保员工能够获取和传达需要通过信息和沟通体系实施的内部控制的相关信息，并且能够管理信息沟通活动的进行；
- **风险评估**——识别并系统分析可能阻碍实现运营活动中内部控制目标的相关风险，从而形成合理的风险应对策略；
- **监控活动**——监控整个内部控制程序并在必要时实施纠正措施；在条件允许的情况下，调整相应的控制程序，以确保内部控制系统的及时响应。
- **控制活动**——制定并实施各类政策、程序、标准和工作指引，以确保管理层设计的控制能够有效应对风险、实现实体的控制目标并有效运行。

这五个要素简要描述如下。

1. 控制环境

阿里云作为阿里巴巴集团的一个业务板块，在组织层面上与阿里巴巴集团（“阿里巴巴”或“集团”）的整体控制环境保持一致。阿里巴巴管理层确立了阿里人的核心价值观以及组织和意识基调。总体控制环境反映了阿里云管理层和员工对内部控制以及支持控制有效性的活动的态度和意识，并且确立了控制活动对组织的重要性以及员工对组织政策、程序和标准的重视程度。为确定和实施内部控制，阿里云制定了与集团一致的核心价值观和行为守则，明确定义了组织架构以及每个部门的角色和职责，并在内部制定了各类政策、程序和标准并进行了妥善传达。

阿里云明确定义了组织架构及各个部门。每个部门的角色和职责均在组织层面分配给各个部门。

阿里云遵循集团的员工招聘、入职和培训计划。按照政策和程序建立了正式机制，以实现人力资源管理的要求。

2. 信息和沟通

阿里云按照既定政策和程序搭建了内部和外部沟通渠道，旨在确保阿里云与其员工以及阿里云与其客户之间的有效沟通。

3. 风险评估

阿里云构建了风险管理框架，以识别、分析和管理公司内部风险以及与所提供服务有关的风险。该风险管理框架涉及管理人员和执行人员，涵盖多项战略风险和运行风险，包括安全性、可用性和保密性风险。

阿里云根据 ISO/IEC 27001:2013 标准和相关行业标准构建了全面的信息安全管理体系。信息安全风险评估必须每年进行一次，具体包括风险识别、分类、威胁监控与分析、控制措施评估以及风险处置等。

阿里云信息数据中心团队负责维护每个数据中心的风险清单，并将风险清单传达给相应的风险管理人员。

4. 监控活动

阿里云每年开展一次全面的系统性信息安全管理检验和评估，旨在评估信息安全政策、标准和要求的执行情况以及安全控制措施的适用性。此外，阿里云的信息安全管理会定期接受内部审计。此类审计旨在验证信息安全政策合规性和控制的运行有效性。审计结果将直接报告给管理层。

IV. 控制活动

阿里云为了规划控制活动而制定了各项政策、程序、标准和工作指引，旨在达到适用的信任服务标准。阿里云的内部控制要素包括对组织或特定程序和应用程序具有广泛影响的控制。

1. 信息安全治理与风险管理

阿里云制定了用于治理和管理信息安全和 IT 运行风险的一系列政策和程序，旨在为所有部门和全体工作人员提供日常工作和管理程序方面的指导。员工可在阿里云内部平台上查阅此类政策。

2. 人力资源

阿里云针对人力资源管理制定了政策和行为准则。新员工须签署劳动合同、保密协议和声明书，其中明确规定了员工在信息安全方面的责任和义务。

阿里云已通过内部门户网站记录和维护了有关其员工的角色和职责及其汇报关系的信息，此信息面向全体员工开放。定期进行绩效评估。任何员工违反信息安全和行为守则要求的行为都将在内部门户网站上进行公布，并给出相应的处罚决定。

阿里云已制定符合集团关于行为守则、信息和数据安全要求的培训计划。

3. 数据安全管理

阿里云已建立数据安全生命周期管理流程，以确保数据安全在整个数据生命周期（包括数据采集、传输、处理、交换、存储和销毁）中得到有效的管理和控制。按照《阿里巴巴集团数据安全规范(总纲)》中定义的相关要求设计和实施安全措施和控制机制。此外，还建立并实施了与数据备份和冗余相关的控制。制定了监控流程，以确保相应控制设计和实施的有效性。

4. 基础设施和虚拟化安全

阿里云的基础设施安全措施和虚拟化技术确保内部网络和物理服务器得到安全保护。阿里云通过计算虚拟化、存储虚拟化和网络虚拟化，来防止租户的云资源被未授权访问，并确保云计算环境下多租户之间的隔离。

阿里云建立了操作系统和镜像加固的相关加固标准。阿里云服务器采用的操作系统和镜像必须按照标准进行配置。

5. 账号和访问控制管理

阿里云的账号和访问控制管理遵循访问控制管理规定所述的最小授权原则和职责分离原则，确保对阿里云环境中的资源和系统的访问得到适当的管理和限制，以防止信息资产受到未授权访问。

制定了账号和访问管理相关的政策和程序，以管理账号的创建、修改和删除。执行定期访问审核，以确保员工访问的适当性。将密码策略嵌入账号管理平台，以防止员工设置简单密码。

6. 资产管理

阿里云对信息资产进行识别、记录、分类和管理，以确保用于提供云服务的信息资产得到合理的保护。制定了相关政策和程序，以规范信息资产的识别、分类和管理。另外，阿里云也制定了相应的指南用于规范信息资产的采购、部署和处置流程。采购新资产必须得到适当人员的授权。在将任何新资产部署到生产环

境之前，应进行测试并记录测试结果。申请将资产转移出数据中心需要经过适当的审批，被转移的资产应在获得批准后适当销毁。

7. 客户身份验证和访问管理

阿里云为客户提供用户身份管理和资源访问控制服务，使客户能够安全管理其资源的访问权限，并有效限制对客户环境的访问权限。

阿里云在其官网上发布了网站服务协议，其中定义了客户和阿里云在客户环境访问管理方面各自承担的责任和义务，包括阿里云提供的服务水平以及关于保密性和数据披露的条款。在阿里云账号注册流程中，客户必须同意并确认接受服务协议。客户成功在阿里云网站注册后会获得唯一的阿里云账号。客户进行自助密码重置时需要通过经验证的手机上的收到的短信验证码验证身份。

资源访问管理(RAM)是阿里云为客户提供的集中式用户身份管理和资源访问权限控制服务。RAM 使得一个阿里云账号（主账号）可拥有多个独立的子用户（RAM 用户）。通过使用 RAM，用户可以在其云账号下为其企业员工、系统或应用程序创立多个独立的 RAM 用户账号，并可以控制这些用户对其云资源的操作权限。每个 RAM 用户都可使用独立的登录密码或访问密钥登录阿里云控制台或以程序的方式调用服务 API 对云资源进行操作，从而避免了共享阿里云账号带来的安全问题。默认情况下，新创建的 RAM 用户账号没有任何资源操作权限，客户可根据最小授权原则为不同的 RAM 用户分配操作权限。

任何阿里云运维人员如果需要临时访问客户的资源，都必须经过客户的身份验证和授权。

8. 加密和密钥管理

阿里云采用最先进的加密技术有效地管理加密和密钥，确保敏感数据的保密性、真实性和完整性。已制定相关政策和指南，用以对敏感数据采取包括加密在内的保护措施。

密钥管理服务 (KMS) 是由阿里云提供的安全管理服务，提供密钥的安全托管、密码运算等基本功能，内置密钥轮换等安全实践，同时支持其他云产品通过一方集成的方式对云产品管理的用户数据进行加密保护。

阿里云对于数据安全提供了全链路的加密保护能力，包括传输加密、存储加密，以及基于硬件的加密计算环境。同时，阿里云提供了基于硬件加密机的加密服务和 SSL 证书服务，为用户提供一整套数据加密的解决方案。

9. 物理和环境安全

阿里云制定了关于物理和环境安全管理的规章制度，以规范安全访问管理和环境控制。访问授权遵循最小特权原则

阿里云数据中心配备了必要的环境保护以及监控控制和机制，以确保物理环境安全。定期监控和评估数据中心服务提供商的表现。

10. 终端安全

阿里云制定了相关的政策和程序以规范移动设备的管理，包括软件安装、防病毒软件、数据泄露防护与网络准入，以防止因移动设备的不当管理或使用引发安全事件和漏洞进而对生产系统造成影响。此外，还制定了控制和技术措施，以管理和监控 员工自带设备(BYOD) 和防病毒软件的安装，从而确保终端安全。还制定了数据泄露防护 (DLP) 解决方案，以监控终端的数据安全。

11. 威胁和漏洞管理

阿里云的威胁和漏洞管理通过检测系统漏洞和未授权操作，并及时采取补救或缓解措施来确保阿里云及其客户环境的安全。阿里云已制定相关政策和指南，以规范安全漏洞的管理，包括安全漏洞的分类和响应机制。按照相关政策和指南中的要求运行威胁和漏洞管理流程。安全部门工作人员会跟踪网络监控系统发现的任何异常操作并进行妥善跟踪处理。每天扫描云平台，并在漏洞管理平台上收集和监控扫描结果。

12. 安全事件管理

阿里云的安全事件管理通过监控和检测安全事件并针对这些事件及时执行适当的响应来确保云平台上的安全操作和保护系统。阿里云建立了安全事件响应标准和指南，以规范安全事件的分类、上报和通知流程。阿里云对云平台的安全进行监控，旨在及时发现平台自身的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。在云平台上的操作日志被日志平台收集后，会分别导入实时计算平台和离线计算平台。各个计算平台通过安全监控算法模型对日志进行处理和分析，以进行异常分析和检测。安全团队负责分析和跟踪事件，并协调相关人员对事件做出响应。已确认的安全事件（如有）会通过多个沟通渠道通知受影响的客户。

13. 故障管理

阿里云建立了故障管理标准和程序，以规范故障的分类和响应要求，以及根据风险等级的故障上报和解决流程，以确保故障得到及时的识别、评估、上报和解决。已开发并利用故障管理平台来识别、整合、跟进和监控通过不同渠道发现的故障。责任人员将及时跟进故障情况。将通过多个沟通渠道通知受影响的客户。

14. 变更管理

阿里云建立了标准化的变更管理流程，以确保云平台上的所有变更在投放到生产环境前都依据相关的制度和流程都得到记录、评估、测试、审批和通报。已就变更管理流程建立并实施访问控制，以确保对生产系统的访问遵循最小特权和职责分离规则。已实施开发、测试和生产的分离环境，并控制对不同环境的访问以仅限授权人员可以访问。

阿里云为云上产品定制的云产品安全生命周期旨在将安全融入到整个产品开发生命周期的各阶段，从而有效地提高云产品的安全能力并降低安全风险。为确保产品的安全性能能够满足云计算的严格要求，SPLC 在

产品立项、安全架构审核、安全开发、安全测试审核、应用发布和应急响应的各个环节层层把关，每个节点都有完整的安全审核机制。

15. 业务连续性管理

阿里云就业务连续性管理制定了一系列阿里云政策和指南，以确保在中断情况下及时恢复关键业务运行。已制定业务连续性计划，并每年对其进行测试。

阿里云遵循容量预测、计划和监控的既定程序，以避免容量瓶颈的发生。阿里云建立了容量管理基线，并评估了由容量限制导致可用性受损的风险。实时监控容量，并在预测用量超过容量容限时采取跟进措施。

服务水平协议中定义和承诺了服务可用性等级，该协议在官方网站上向客户公开提供。

16. 供应商管理

阿里云已制定相关政策和程序，以规范现场工作开展之前、期间和之后对供应商和第三方员工的管理，从而确保第三方服务提供商达到商定的安全和服务交付水平。

所有供应商在签约前都必须通过阿里云的背景调查，并需要签署合同和保密协议。所提供的服务应接受定期评估。

17. 审计和合规

阿里云已围绕审计和合规管理制定政策和程序，以持续监控内部控制、确保对高安全标准和质量的承诺、维护有效证书和认证，并遵守相关法律、法规和合同要求。

根据管理层审核并批准的审计计划，至少每年开展一次内部审计。内部审计团队会定期跟进内部审计中发现的问题，并在控制环境和体系中引入纠正和预防措施。

阿里云致力于持续改进其内部控制系统，以满足新的行业标准。阿里云在全球运营和维护，遵守国际信息安全标准，也遵守提供云产品和服务的地域内的信息安全标准。阿里云致力于遵循国际最佳实践，并定期独立验证是否符合行业标准。更多信息请参见阿里云安全和合规中心。

18. 补充用户机构控制

在责任共担模式下，位于阿里云中的应用和数据的安全性由阿里云及其客户共同负责。在设计系统时，阿里云考虑到用户机构会实施特定补充控制，以满足适用的信任服务标准。仅凭阿里云控制无法有效地满足适用的信任服务标准。因此，各用户机构的内部控制必须与阿里云控制一起评估。

本节重点描述了阿里云认为应由用户机构（即客户）负责的控制领域。因此，这些补充控制应由用户机构考虑和开发。以下控制列表描述了客户可能需要执行的额外政策、程序和控制，以满足只有在合理设计和有效运行补充控制的情况下才能满足的适用的信任服务标准。各用户机构必须评估自己的内部控制组合，以确定控制是否设计合理且有效运行。下表不是（也不意图作为）包含为用户机构提供基础的控制完整列表。为了实现有效管理，用户机构可能还需要根据其具体情况引入其他必要的控制活动。

域	适用产品	用户机构（即客户）的责任
组织安全	全部	• 用户机构在设计针对阿里云上应用和数据的补充控制时，应制定风险管理流程和评估控制目标以应对风险。 • 用户机构应制定政策、程序和标准以指导组织内信息安全管理和运行。 • 用户机构应建立补充控制的监控机制，以评估补充控制的设计和运行有效性。
应用控制	全部	• 用户机构应实施适当控制，以确保应用级控制（例如职责分离、自动控制、系统计算、报告生成、系统接口）的设计和运行有效性。
访问安全	全部	• 用户机构应实施访问控制，例如安全组、RAM 角色和访问控制清单以保护其云实例。 • 通过所提供的联系信息验证用户身份（例如，当用户机构为其云账号执行自助密码重置时采用短信验证码）。因此，用户机构应实施相关控制，以确保阿里云所需的联系信息（例如手机号）得到准确注册和及时更新，并确保验证渠道（例如手机和电子邮件）安全。 • 用户机构应使用多重身份验证方法来访问其云资源。制定密码策略时应考虑密码策略的复杂性。 • 访问密钥应妥善保护和保密。 • 用户机构应实施强化的实例防火墙策略。 • 用户机构应确保实施适当的安全配置，以支持用户身份验证系统的完整性并防止越权访问。 • 用户机构应实施访问控制，以保护其自定义镜像免受越权访问。 • 用户机构应制定网络安全标准，并确保其虚拟专用网只连接到适当的内部网络。 • 用户机构应实施控制，以确保仅将已授权且安全的更新应用于安全组规则，从而保障自己的不同 ECS 实例的访问安全性。

		• 用户机构应制定和维护 IP 白名单，以保护用户机构的实例免受越权访问。 • 用户机构应为存储访问建立有效的访问控制，以保护 bucket 和对象免受越权访问。 • 用户机构应定期审核对其云资源的访问和授权 IP。 • 用户机构应针对敏感活动、系统错误、数据更改等情况，启用和配置适用的记录功能，以支持监控控制和事件响应流程。
	仅物联网产品	• 用户机构应实施适当的访问控制，以确保自己的物联网设备、服务器和网关终端的安全。 • 用户机构应实施适当的访问控制，以确保自己开发的物联网固件升级包的本地安全。
数据安全	全部	• 如果使用阿里云提供的数据传输服务，用户机构应实施适当的控制，以确保考虑到跨境数据传输要求。 • 用户机构应在与阿里云的所有交互中使用加密 (TLS/SSL) 连接。对数据传输安全级别有较高要求的用户机构（例如，要求 PCI DSS 合规）应采用 TLS 1.2。必要时，用户机构应设计其所需的 CMK 轮换。 • 用户机构应根据具体要求实施和维护加密选项。
	仅物联网产品	• 用户机构应针对自己的物联网设备、应用、服务器和网关终端之间传输的数据评估和实施适当的保护措施。 • 用户机构应实施适当的控制，以确保敏感数据（例如下载到本地的 deviceSecret）的安全，以及本地存储的其他数据的安全。
变更管理	全部	• 用户机构应为自己在阿里云上托管的应用和数据实施适当的变更管理控制。 • 用户机构应确保在必要时将最新补丁应用于其实例。 • 用户机构应设置分离的环境和用户账号，使生产系统与开发活动彼此隔离。
	仅物联网产品	• 用户机构应实施适当的变更管理控制，以确保阿里云所提供的软件（包括 SDK、移动应用、AliOS 产品等）在重新开发期间的安全，并确保及时的安全补丁升级。

问题管理	全部	• 用户实体应向阿里云告知特定于阿里云所提供产品和服务的任何故障或安全事件，并支持阿里云的及时事件响应流程。
业务连续性管理	全部	• 用户机构应根据其需求制定适当的备份和恢复策略和计划。应测试这些策略和计划以确保其有效性。阿里云提供客户数据备份功能，用户机构可建立相应的机制，以实现及时备份和恢复。 • 用户机构应根据其需求制定灾难恢复计划和《业务连续性计划》。应定期进行演练测试。 • 用户机构应利用多可用区和多区域选项，并设计和实施冗余系统，以确保所需的冗余级别和高可用性架构。
	仅物联网产品	• 阿里云在其物联网产品和服务系统中提供设备监控的功能。用户机构应实施适当的控制，以监控自己的物联网设备和网关的状态。 • 用户机构应实施适当的控制，以确保有效备份自己的物联网设备和网关所存储的数据。