Alibaba Cloud

系统和组织控制 1（SOC1）报告

类型 II

阿里云公共云服务体系报告

报告期间：2020 年 10 月 1 日至 2021 年 9 月 30 日

目录

第一节——独立服务审计师报告（翻译自英文版本）

独立服务审计师报告（翻译自英文版本）

致阿里云计算有限公司管理层：

范围

我们根据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、阿里云美国有限公司、阿里云（印度）有限公司、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“服务机构”或“阿里云”）的认定（“该认定”）中识别出的标准，检查了阿里云对在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间用于提供云服务的云服务体系（“体系”）的描述“阿里云对其云服务体系的描述”（“该描述”）以及在该描述中所述的，为实现相关控制目标的控制的设计适当性和运行有效性。该描述中所包含的控制及控制目标是指服务机构管理层认为很可能与用户机构财务报告内部控制相关的控制，且该描述未涵盖那些与用户机构财务报告内部控制不相关的云服务体系的部分。

第五节“服务审计师报告中未涵盖的阿里云提供的其他信息”中包含的信息由服务机构的管理层列示，以提供额外信息，但不属于阿里云对其云服务体系的描述的一部分。第五节中关于服务机构的信息不在对云服务体系的描述以及为实现该描述中所述相关控制目标的控制的设计适当性和运行有效性的检查程序范围内。

描述中指出，仅当设计服务机构的控制时假定的用户机构的补充控制，随服务机构的相关控制一起设计适当且有效运行时，描述中所指定的某些控制目标才能实现。我们的检查并不延伸至用户机构的补充控制，且我们未对此类用户机构的补充控制的设计适当性或运行有效性进行评估。

服务机构的责任

在第二节中，服务机构已就该描述的公允表达以及为实现该描述中所述相关控制目标的控制的设计适当性和运行有效性提供了认定。服务机构负责编制该描述及其认定（包括该描述及其认定的完整性、准确性和列报方式），提供该描述中所涵盖的服务，说明控制目标并在该描述中陈述控制目标，识别影响控制目标实现的风险，选择认定中所述标准，以及设计、执行和记录用以实现该描述中所述的相关控制目标、且设计适当并有效运行的控制。

服务审计师的职责

我们的责任是基于我们的检查，对该描述的公允表达以及为实现该描述中所述相关控制目标的控制的设计适当性和运行有效性发表意见。

我们根据美国会计师协会颁布的鉴证准则执行本检查。这些准则要求我们计划和执行检查，以就对在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间，基于管理层认定的标准，在所有重大方面，该描述是否公允表达、以实现描述中所述的相关控制目标的控制的设计是否适当和运行是否有效，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。

对服务机构的体系的描述，以及为实现该描述中所述相关控制目标的服务机构控制的设计适当性和运行有效性所进行的检查，涉及以下程序：

- 实施程序以获取关于基于管理层认定的标准的该描述的公允表达以及为实现该描述中所述相关控制目标的控制的设计适当性和运行有效性的证据。

- 评估该描述未被公允表达以及为实现该描述中所述相关控制目标的控制的设计不适当或未有效运行的风险。
- 测试管理层认为必要的控制的运行有效性，以提供实现该描述中所述相关控制目标合理保证。
- 评估该描述的总体表达、其中所述控制目标的适当性以及服务机构在其第二节认定中指定的标准的适当性。

固有限制

该描述是为了满足广泛范围内的用户机构以及对其财务报表进行审计并出具报告的审计师的共同需求而编制，因此可能并未包括个别用户机构认为对其自身特定环境重要的体系的每一个方面。由于其性质，服务机构或分包服务机构的控制可能无法防止或发现并纠正提供云服务中的所有错报。此外，根据对该描述表达公允性的任何评估或者关于控制就实现相关控制目标的设计适当性或运行有效性的任何结论来推断未来期间的状况，将面临服务机构或分包服务机构的控制可能变得无效的风险。

对控制测试的描述

第四节中对所测试的特定控制以及这些测试的性质、时间和结果予以详述。

意见

我们认为，基于第二节中阿里云的认定中所述的相关标准，在所有重大方面：

a. 该描述公允地表达了在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间设计和实施的体系；

b. 与该描述中所述的控制目标相关的控制的设计适当，为以下陈述提供合理保证：如果所描述的控制在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间有效运行且用户机构应用了服务机构的控制设计中假定的补充控制，则可以实现指定的控制目标。

c. 相关控制在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间有效运行，为以下陈述提供合理保证：如果在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间用户机构有效运行在服务机构的控制设计中假定的补充控制，则可以实现指定的控制目标。

其他事项

此版本报告是基于原始版本（以英文版出具）的译文。在所有关于信息、观点或意见的解释中，如有任何差异，以原始英文版报告为准。

限制用途

本报告（包括第四节中对控制测试及其结果的描述）仅供阿里云管理层、以及在 2020 年 10 月 1 日至 2021 年 9 月 30 日部分或全部期间使用阿里云的云服务体系的用户机构、以及对用户机构财务报表或财务报告内部控制进行审计并出具报告的审计师使用。用户机构及其独立审计师应充分理解在评估用户机构财务报表的重大错报风险时，必须将此报告与其他相关信息（包括关于由用户机构自身运行的控制的信息）一同考虑。本报告不得也不应当被除这些特定方以外的其他方使用。如果在 2020 年 10 月 1 日至

2021 年 9 月 30 日期间未与阿里云签订服务合同的用户机构或其独立审计师（以下统称为非特定方）获得本报告，则使用本报告所产生的任何后果以及相关风险由该非特定方单独承担责任。非特定方不可依赖本报告，并就此对罗兵咸永道会计师事务所主张任何权利。此外，罗兵咸永道会计师事务所不会对获得本报告的非特定方承担任何责任或义务。

罗兵咸永道会计师事务所

中国香港

2021 年 11 月 15 日

第二节——阿里云管理层关于云服务体系的认定

Alibaba Cloud

2020 年 10 月 1 日至 2021 年 9 月 30 日期间阿里云管理层关于云服务体系的认定

我们编制了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、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“服务机构”或“阿里云”）在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间用于提供云服务的云服务体系（“体系”）的描述“阿里云对其云服务体系的描述”（“该描述”），该描述是针对在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间使用该体系的用户机构，以及对其财务报表或财务报告内部控制进行审计并出具报告的审计师。用户机构的独立审计师应充分理解在评估用户机构财务报表的重大错报风险时，应将此报告与其他相关信息（包括关于由用户机构自身运行的控制的信息）一同考虑。

该描述指出，仅当设计阿里云的控制时假定的用户机构的补充控制，随阿里云的相关控制一起设计适当且有效运行时，描述中所指定的某些控制目标才能实现。描述并不延伸至用户机构的控制。

兹就我们所知及所信，我们确认

a. 该描述公允表达了在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间用户机构所使用的用于提供云服务的云服务体系，这涉及到可能与用户机构财务报告内部控制相关的控制。做出这一认定的标准如下：

   i. 该描述反映了供用户机构使用的用于提供云服务的云服务体系是如何设计和实施的，包括，如适用

      (1) 提供的服务的类型。

      (2) 提供这些服务的自动系统以及人工系统的程序。

      (3) 用于实施程序的信息，包括错误信息的更正以及信息如何被转化到为用户机构编制的报告和其他信息。

      (4) 体系如何获取和处理重大事件和情况。

      (5) 为用户机构编制报告和其他信息的流程。

      (6) 由分包服务机构执行的服务，如有，包括采取的是分拆法还是总括法。

      (7) 相关的控制目标以及为实现这些目标而设计的控制，包括，在适当情况下，服务机构在控制设计中所假定的那些用户机构的补充控制和分包服务机构的补充控制。

      (8) 与提供的服务相关的控制环境、风险评估流程、信息与沟通（包括相关业务流程）、控制活动和监督活动的其他方面。

   ii. 包含描述所覆盖期间服务机构的体系变化的相关细节。

iii. 没有遗漏或者曲解与服务机构体系相关的信息，同时我们认可这些描述是为了满足广泛范围内的用户机构及其独立审计师的共同需求而编制的，因此可能并未包括个别用户机构及其审计师认为对其自身的特定环境重要的云服务体系的每一个方面。

b. 在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间，如果用户机构采用了设计阿里云的控制时所假定的补充控制，所附描述中所述的与控制目标相关的控制在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间内设计适当并运行有效。做出这一认定采用的标准如下

i. 影响描述中所述的控制目标实现的风险已被服务机构的管理层识别。

ii. 描述中所识别的这些控制，如果有效运行，可以合理保证这些风险不会阻止描述中所述的控制目标的实现。

iii. 这些控制按照既定设计得以一贯执行，包括由具有适当能力和授权的人执行的人工控制。

阿里云计算有限公司

2021 年 11 月 15 日

第三节——阿里云对其云服务体系的描述

2020 年 10 月 1 日至 2021 年 9 月 30 日期间阿里云对其云服务体系的描述

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。阿里云云服务由自主开发的云服务平台和技术提供支持。通过大力投资技术创新以不断提升所提供的计算能力和规模经济效应，阿里云旨在打造全球领先的云计算基础架构。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领域提供物联网平台。阿里云致力于打造物联网基础结构。至关重要的是物联网平台提供的数据存储和处理能力能够支持应用程序编程接口（API）和其他阿里云服务的集成，从而使阿里云物联网平台的用户获得一套综合性的服务。物联网平台标志性的规则引擎拥有快速数据采集、存储和应用程序开发的能力。通过建立覆盖整个行业的集成式云端和设备终端开发平台、搭建一条完整的物联网产业链以及建立全球适用的物联网标准，阿里云致力于持续性地建设物联网生态系统、平台和基础设施，以加速实体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公共、安全和开放的云计算服务平台。本报告涵盖以下公共云服务：

1. 操作审计
2. 容器服务 ACK
3. 云解析 DNS
4. 云解析 PrivateZone
5. 阿里云 Elasticsearch
6. 消息队列 for Apache RocketMQ
7. 阿里云工业互联网
8. 云原生数据仓库 AnalyticDB MySQL 版
9. 云原生数据仓库 AnalyticDB PostgreSQL 版
10. DDoS 防护
11. API 网关
12. 应用配置管理
13. 应用实时监控服务
14. 云效
15. 云数据库 HBase 版
16. 云数据库 MongoDB 版
17. 云数据库 OceanBase 版
18. 云数据库 Redis 版
19. 云数据库 RDS MySQL 版
20. 云数据库 RDS PostgreSQL 版

21. 云数据库 RDS PPAS 版
22. 云数据库 RDS SQL Server 版
23. 视频直播
24. 弹性伸缩
25. 运维安全中心（堡垒机）
26. 块存储
27. CDN
28. 配置审计
29. 云企业网 CEN
30. 云防火墙
31. 漏洞扫描
32. 云虚拟主机
33. 云监控
34. 容器镜像服务
35. 内容安全
36. 加密服务
37. 数据管理
38. 数据传输服务 DTS
39. 数据库备份
40. 智能数据构建与管理 Dataphin
41. DataV
42. DataWorks（数据工场）
43. 数据库审计
44. 全站加速
45. 专有宿主机
46. 邮件推送
47. 弹性裸金属服务器（神龙）
48. 云服务器 ECS
49. 弹性容器实例
50. GPU 云服务器
51. 弹性高性能计算 E-HPC
52. 弹性公网 IP
53. E-MapReduce
54. 企业级分布式应用服务 EDAS
55. 高速通道
56. 文件存储 NAS
57. 风险识别
58. 函数计算
59. 混合云备份服务
60. 应用身份服务
61. 智能语音交互

62. 物联网平台
63. 密钥管理服务
64. 物联网设备身份认证
65. 物联网边缘计算
66. 生活物联网平台(天猫精灵 IoT 平台)
67. IoT 设备安全运营中心
68. 物联网智能视频服务
69. 物联网络管理平台
70. 日志服务
71. 机器学习
72. 大数据计算服务 MaxCompute
73. 消息队列 Kafka 版
74. NAT 网关
75. 对象存储 OSS
76. 印刷文字识别
77. 运维编排
78. 云原生关系型数据库 PolarDB
79. 智能分析套件 Quick BI
80. 实时计算 Flink 版
81. 访问控制
82. 资源管理
83. 安全加速 SCDN
84. 云安全中心
85. 敏感数据保护
86. 负载均衡（SLB）
87. 短信服务
88. 轻量应用服务器
89. 超级计算集群
90. 表格存储
91. 专有网络 VPC
92. VPN 网关
93. Web 应用防火墙（WAF）

本报告将报告涵盖的阿里云公共云服务分为以下大类，并提供每种云服务的简要介绍。阿里云官方网站列有可供客户使用的所有阿里云服务。客户应查阅相应的阿里云官方网站文档以获取更多信息。

分析

阿里云 Elasticsearch：阿里云 Elasticsearch 是一项云上服务，集成了 Elasticsearch、Kibana 以及阿里云 VPC、云监控、访问管控等功能，用于数据分析、数据搜索等场景服务。

智能数据构建与管理 Dataphin：Dataphin 旨在面向各行各业大数据建设、管理及应用诉求，提供一站式的从数据接入到数据消费全链路的智能数据构建与管理的大数据能力， 包括产品、技术和方法论等，助力打造标准统一、融会贯通、资产化、服务化、闭环自优化的智能数据体系，以驱动创新。

DataV 数据可视化：DataV 数据可视化是一款一站式的数据可视化应用搭建工具，集可视化图表制作、数据连接配置、一键部署发布于一体，用户只需在图形化的编辑界面进行简单的拖拽、点击等操作，即可制作出实时数据驱动的炫酷可视化应用。帮助非专业的工程师通过图形化的界面轻松搭建专业水准的可视化应用，满足会议展览、业务监控、风险预警、地理信息分析等多种业务的展示需求。

DataWorks（数据工场）：DataWorks 是阿里云推出的大数据领域平台级产品，提供一站式大数据开发、数据权限管理、任务离线调度，等功能。底层依赖阿里云自主研发的海量数据计算引擎 MaxCompute，提供海量任务的离线加工、分析、云数仓搭建、大数据挖掘等应用于多种场景的功能。‘开箱即用’的使用方式，让用户无需再过多关心底层集群的搭建和运维所带来的成本和繁琐。

E-MapReduce：E-MapReduce（EMR）是在阿里云平台上运行的一种大数据处理解决方案。EMR 是构建于云服务器 ECS 实例上的基于开源 Apache Hadoop 和 Apache Spark 的产品。用户可以方便地使用 Hadoop 和 Spark 生态系统组件分析和处理数据。用户还可以通过 E-MapReduce 将数据非常方便地处理阿里云其他的云数据存储系统的数据，如 OSS、SLS、RDS 等。

大数据计算服务 MaxCompute：云原生大数据计算服务（MaxCompute，原名 ODPS）是一种快速、完全托管的 TB/PB 级数据仓库解决方案。MaxCompute 向用户提供了完善的数据导入方案以及多种经典的分布式计算模型，能够更快速的解决用户海量数据计算问题，有效降低企业成本，并保障数据安全 。

智能分析套件 Quick BI：Quick BI 提供海量数据实时在线分析服务，支持拖拽式操作、丰富的可视化效果，可以帮助用户轻松自如地完成数据分析、业务数据探查、报表制作等工作。它不仅是业务人员查看数据的工具，更是数据化运营的助推器。

实时计算 Flink 版：实时计算是基于 Apache Flink 构建的一站式、高性能实时大数据处理平台，广泛应用于流式数据处理、离线数据处理、DataLake 计算等场景。阿里云实时计算助力企业向实时化、智能化大数据计算升级转型。

人工智能

智能语音交互：智能语音交互适用于多个应用场景中，包括智能问答、智能质检、实时演讲字幕、访谈录音转写等场景，在金融、保险、电商、智能家居等多个领域均有应用案例。智能语音交互使用户可以使用自主学习平台等工具改善语音识别效果，而且提供了功能更丰富的管理控制台和更易用的 SDK。

机器学习：阿里云机器学习打造一站式人工智能平台，为用户提供机器学习服务，其中包括数据预处理、特征工程、模型训练、模型预测、模型评估。

印刷文字识别：印刷文字识别（OCR）将图片中的文本转换为可编辑的文本。印刷文字识别（OCR）支持十多种应用场景的文本转换，包括普通文本、个人驾照、身份证件、发票、教育考试、车辆物流文件、办公文件、企业证书、小语种文件、自定义模板等。

容器与中间件

消息队列 for Apache RocketMQ：消息队列 for Apache RocketMQ 是由阿里巴巴自研的分布式消息队列服务，由阿里云平台完全托管，能够在微服务、分布式系统和无服务应用程序之间，提供基于消息的可靠异步通信机制，轻松构建松耦合、可扩展、高可用分布式系统。消息队列 for Apache RocketMQ 服务具备低延迟、高并发、高可用、高可靠、可支撑万亿级数据洪峰和超强消息堆积能力，借助 AlibabaMQ，用户可以在任意规模的应用组件之间自由地传递数据。

应用配置管理：应用配置管理（Application Configuration Management，简称 ACM）是一款应用配置中心产品，其前身为淘宝内部配置中心 Diamond。基于该产品，用户可以在微服务、DevOps、大数据等场景下极大地减轻配置管理的工作量，增强配置管理的服务能力。

应用实时监控服务：业务实时监控服务 (Application Real-Time Monitoring Service, 简称 ARMS) 是一款阿里云 APM 类监控产品。用户可以基于该产品的前端、应用监控，迅速便捷地构建实时响应的业务监控能力。

企业级分布式应用服务 EDAS：企业级分布式应用服务（Enterprise Distributed Application Service, 简称 EDAS）是阿里云企业级互联网架构解决方案的核心产品，作为阿里云分布式服务架构的重要组成部分，EDAS 提供了包括应用生命周期管理和发布运维在内的丰富的功能。EDAS 全面兼容 Apache Tomcat 的 Java 容器，提供高性能的分布式服务框架以及秒级推送的分布式配置管理服务。此外，EDAS 还创新性的提供了分布式系统链路追踪、容量规划、数据化运营和多款高可用稳定性组件。

消息队列 Kafka 版：消息队列 Kafka 版是阿里云提供的分布式、高吞吐、可扩展的消息队列服务，为用户提供增强型全托管 Apache Kafka 集群服务，使用户免于集群配置、故障运维、补丁升级、数据持久化、弹性伸缩、资源管控、监控报警等基础设施难题。

数据库

云原生数据仓库 AnalyticDB MySQL 版：云原生数据仓库 AnalyticDB MySQL 版（AnalyticDB for MySQL）是一种高并发低延时的 PB 级实时数据仓库，具有简单易用、高性能、安全稳定的特点。云原生数据仓库 AnalyticDB MySQL 版（AnalyticDB for MySQL）支持用户便捷地构建在线统计报表、多维分析服务和实时数据仓库。云原生数据仓库 AnalyticDB MySQL 版采用分布式计算架构，利用云端的弹性伸缩能力，能对百亿条甚至更大量级的数据进行实时计算。

云原生数据仓库 AnalyticDB PostgreSQL 版：云原生数据仓库 AnalyticDB PostgreSQL 版是一个大规模在线数据仓库服务，具有实时、易用、海量扩展的特点。 AnalyticDB for PostgreSQL （原 HybridDB for PostgreSQL）基于开源数据库 Greenplum 构建，由阿里云深度扩展，兼容 ANSI SQL 2003，同时

兼容 PostgreSQL/Oracle 数据库生态，支持行存储和列存储模式，即提供高性能离线数据处理，也支持高并发在线查询。

云数据库 HBase 版： 云数据库 HBase 版是一个 100%兼容开源 HBase 并深度扩展，稳定、易用、低成本的 NoSQL 数据库。云数据库 HBase 版融合了 Spark、Phoenix、Solr 等生态技术，提供稳定、易用、低成本的服务，提供海量数据的实时存储、高并发吞吐、轻 SQL 分析、全文检索、时序时空查询等能力。

云数据库 MongoDB 版：阿里云云数据库 MongoDB 版是一种安全可靠、可弹性伸缩的云数据库服务，目前支持 ReplicaSet 和 Sharding 两种部署架构，通过简单的几步操作即可快速部署。阿里云云数据库 MongoDB 版是一种高度可用的托管服务，具有自动监控、备份及容灾功能。

云数据库 OceanBase 版： 云数据库 OceanBase 版是一款金融级的分布式关系数据库，具备高性能、高可用、强一致、可扩展和兼容性高等典型优势，适用于对性能、成本和扩展性要求高的金融场景。

云数据库 Redis 版：阿里云数据库 Redis 版是兼容开源 Redis 协议标准、提供内存加硬盘混合存储的数据库服务，基于高可靠双机热备架构及可平滑扩展的集群架构，可充分满足高吞吐、低延迟及弹性变配的业务需求。阿里云数据库 Redis 版支持主从、集群和读写分离架构，具备低延迟大吞吐且支持弹性扩缩容的特点，提供大热 Key 实时诊断能力。

云数据库 RDS MySQL 版：MySQL 是全球最受欢迎的开源数据库之一，作为开源软件组合 LAMP（Linux + Apache + MySQL + Perl/PHP/Python）中的重要一环，广泛应用于各类应用场景。

云数据库 RDS PostgreSQL 版：云数据库 RDS PostgreSQL 版是一种可弹性伸缩的在线数据库服务，并具备自动监控、备份、容灾恢复等方面的全套解决方案。

云数据库 RDS PPAS 版：云数据库 RDS PPAS 版是一种可弹性伸缩的在线数据库服务，并具备自动监控、备份、容灾恢复等方面的全套解决方案。

云数据库 RDS SQL Server 版：云数据库 RDS SQL Server 版是一种可弹性伸缩的在线数据库服务，并具备自动监控、备份、容灾恢复等方面的全套解决方案。

数据管理： 数据管理（Data Management，简称 DMS）是阿里巴巴自研的数据库研发服务平台，支持超过 23 种数据库类型、多种环境来源统一管理的可视化数据管理平台，免安装、免运维，可帮助企业解决数据访问安全管控、提升企业的数据变更操作安全、提升企业的数据库研发效能。数据管理是一种集数据管理、结构管理、用户授权、安全审计、数据趋势、数据追踪于一体的数据管理服务。用户可以使用数据管理服务实现易用的数据库管理入口，让数据更安全、管理更高效、数据价值更清晰。

数据传输服务 DTS：数据传输服务(Data Transmission Service,DTS)支持关系型数据库 RDBMS、NoSQL、OLAP 等数据源之间的数据迁移同步。提供数据库不停服迁移、实时数据订阅及数据实时同步等多种数据传输方式。通过 DTS，用户可以在源数据库正常运行情况下，平滑地完成数据迁移。同时，用户还可以利用 DTS 进行 RDS 实例间的数据实时同步，有效解决数据异地容灾、减少跨地区访问等业务问题。除此之外，DTS 还支持 RDS 实例增量数据实时订阅，实现轻量级缓存更新、异步消息通知及定制化数据实时同步等业务场景。

数据库备份：数据库备份（Database Backup，简称 DBS）是为数据库提供连续数据保护、低成本的备份服务。数据库备份提供无限容量的备份存储、秒级应急恢复和恢复演练，并借助秒级沙箱实例和备份数据查询激活冷数据。

云原生关系型数据库 PolarDB：PolarDB 是与 MySQL、PostgreSQL、Oracle 引擎兼容的云原生关系型数据库在存储计算分离架构下，利用了软硬件结合的优势，为用户提供具备极致弹性、高性能、海量存储、安全可靠的数据库服务。

开发者服务

云效：云效 Devops 是一个开发人员平台，将 Projects、Thoughts、Flow、Codeup、Packages 和 Testhub 结合在一起支持开发人员的工作。

云监控：云监控可用于收集获取阿里云资源的监控指标或用户自定义的监控指标，探测已订阅服务的可用性，并允许用户针对特定指标设置警报。云监控可以使用户全面了解阿里云上资源的使用情况、业务的运行状况和健康度，并及时收到异常警报并做出反应，保证应用程序顺畅运行。

弹性计算

容器服务 ACK：容器服务 ACK 是助力企业高效运行云端 Kubernetes 容器化应用。容器服务 Kubernetes 版（简称 ACK）整合了阿里云虚拟化、存储、网络和安全能力，为用户提供高性能可伸缩的容器应用管理能力，支持企业级容器化应用的全生命周期管理。

弹性伸缩：弹性伸缩是根据用户的业务需求自动调整计算资源的服务。当对计算资源的需求增加时，弹性伸缩会自动添加 ECS 实例以满足其他用户需求，或在用户请求减少的情况下删除实例。

云虚拟主机: 云虚拟主机是一个虚拟服务器，用于存储和托管网站内容，建立在 ECS 上。

容器镜像服务：容器镜像服务是一个安全的镜像托管平台，提供安全的镜像托管平台，稳定的国内外镜像构建服务，方便用户进行镜像全生命周期管理。

专有宿主机：专有宿主机（DDH）是阿里云专为企业用户提供的全托管服务器托管服务。具有物理资源独享、部署更灵活、配置更丰富、性价比更高等特点。每个租户都不需要与其他租户共享云主机所有物理资源。

弹性裸金属服务器（神龙）：弹性裸金属服务器（神龙）是一款同时兼具虚拟机弹性和物理机性能及特性的新型计算类产品，是基于阿里云完全自主研发的下一代虚拟化技术而打造的新型计算类服务器产品。与上一代虚拟化技术相比，下一代虚拟化技术的主要创新在于，不仅支持普通虚拟云服务器，而且全面支持嵌套虚拟化技术，保留了普通云服务器的资源弹性，并借助嵌套虚拟化技术保留了物理机的体验。

云服务器 ECS：云服务器 ECS（Elastic Compute Service）是阿里云提供的性能卓越、稳定可靠、弹性扩展的 IaaS（Infrastructure as a Service）级别云计算服务。阿里云云服务器 ECS 具有快速内存和最新的 Intel CPU，可帮助用户为云应用程序提供技术支持，并以较低时延实现更快的结果。

弹性容器实例：弹性容器实例（ECI）是 serverless 和容器化的弹性服务，客户无需管理服务器即可运行容器。

GPU 云服务器：GPU 云服务器是基于 GPU 的计算服务，满足用户在深度学习、视频处理、科学计算和可视化等场景中的需求。

弹性高性能计算 E-HPC：弹性高性能计算（EHPC）是端到端公共云服务，为客户提供快捷、弹性、安全和与阿里云产品互通的云超算平台。

函数计算：函数计算是一个事件驱动的全托管计算服务。客户无需管理服务器等基础设施，只需编写代码并上传。函数计算会为用户准备好计算资源，并以弹性、可靠的方式运行代码。

运维编排：阿里云运维编排（OOS）是一个全面的云上自动化运维平台，提供了运维任务的管理和执行。用户可以通过 OOS 管理以及执行一系列的运维工作，例如事件驱动，批量操作，定时运维任务，跨地域等。

轻量应用服务器：轻量应用服务器是面向单机应用场景的新一代计算服务。该服务器提供应用一键部署，支持一站式的域名、网站、安全、运维、应用管理等服务。

超级计算集群：超级计算集群（Super Computing Cluster，SCC）服务器在弹性裸金属服务器基础上，加入高速 RDMA 互联支持，大幅提升网络性能，提高大规模集群加速比，在提供高带宽、低延迟的优质网络的同时，还具备弹性裸金属服务器的所有优点。超级计算集群（Super Computing Cluster，SCC）使用高速 RDMA 网络互联的 CPU 以及 GPU 等异构加速设备，面向高性能计算、人工智能/机器学习、科学/工程计算、数据分析、音视频处理等应用，提供极致计算性能和并行效率的计算集群服务。

企业应用与云通讯

云解析 DNS：云解析 DNS（Domain Name System，简称 DNS）是一种安全、快速、稳定、可靠的权威 DNS 解析管理服务。云解析 DNS 为企业和开发者将易于管理识别的域名转换为计算机用于互连通信的数字 IP 地址，从而将用户的访问路由到相应的网站或应用服务器。

API 网关：API 网关（API Gateway），提供 API 托管服务，涵盖 API 发布、管理、运维、售卖的全生命周期管理。辅助用户简单、快速、低成本、低风险的实现微服务聚合、前后端分离、系统集成，向合作伙伴、开发者开放功能和数据。

邮件推送：邮件推送（DirectMail）是一款简单高效的电子邮件发送服务，它构建在可靠稳定的阿里云基础之上，帮助用户快速、精准地实现事务邮件、通知邮件和批量邮件的发送。

资源管理：阿里云资源管理服务包括一系列支持企业 IT 治理的资源管理产品，它支持用户根据其业务需求建立合适的资源组织关系，且可使用目录、资源文件夹、账户和资源组来组织和管理所有用户的资源。

短信服务：短信服务作为一款覆盖全球的短信服务，具有友好、高效、智能的互联化通讯能力，帮助企业迅速搭建客户触达通道。用户只需调用 API 或者使用群发助手，即可发送验证码、通知类和营销类短信至全球 200 多个国家和地区的手机上。

物联网

阿里云工业互联网：阿里云工业互联网紧密连接并协调工厂设备、生产线、产品、供应链和客户，为公司提供可靠的基础平台和丰富的上层工业应用，并结合全方位的工业支持协助公司完成数字化转型。

物联网平台：物联网企业通过阿里云物联网平台实现设备与物联网平台之间的稳定通信。物联网平台还提供各种安全措施确保单个设备的安全以及设备与物联网平台之间的安全通信。API 和其他阿里云服务的集成也依赖于它的数据存储和处理功能。它还具有高度的可定制性。

物联网设备身份认证：IoT 设备身份认证是一个物联网设备身份认证系统，通过可信计算和密码技术为物联网系统提供设备安全认证、安全连接、业务数据加密、密钥管理等端到端的可信接入能力。

物联网边缘计算：物联网边缘计算继承了云和边缘计算，为阿里云提供原生支持。它与各种物联网应用层数据收集协议兼容，并使云应用能无缝使用边缘功能。

生活物联网平台(天猫精灵 IoT 平台)：生活物联网平台(天猫精灵 IoT 平台)是阿里云 IoT 面向消费者智能设备的物联网平台，解决智能设备中经常遇到的设备连接、App 控制、设备消息推送、语音控制、语音控制等问题。提供全套配置方案，大大降低“设备-云-应用”的开发成本。

IoT 设备安全运营中心：IoT 设备安全运营中心帮助用户识别和缓解安全威胁，确保物联网系统的安全运行。 Link SOC 不仅可以修复设备中发现的安全漏洞，还可以监控所有设备上的操作。异常操作将被预先配置的规则阻止，或触发安全管理员警报以进行后续操作。IoT 设备安全运营中心提供针对安全威胁的持续保护，并将异常操作的影响降至最低。

物联网智能视频服务：物联网智能视频服务是一个提供视频流、存储、转发、播放和 AI 计算云服务的视频云平台，允许视频设备制造商、解决方案提供商和服务提供商将视频设备的数据快速部署到云端并构建视频场景应用。 Link Visual 还为需要数据隐私保护的视频提供安全的数据传输和存储服务。

物联网络管理平台：物联网络管理平台是企业使用物联网服务的网络管理平台，旨在帮助开发者在企业层面构建大容量、高并发的物联网网络。开发者可以将物联网络管理平台与物联网平台结合使用，从各个环节的功能中受益，并拥有一个自我管理的 IoT WiFi 网络。

媒体服务

视频直播：阿里云视频直播服务是基于领先的内容接入与分发网络和大规模分布式实时视频处理技术打造的音视频直播平台，提供易接入、低延迟、高并发、高清流畅的音视频直播服务。

网络

云解析 PrivateZone：阿里云 DNS PrivateZone 是基于 VPC 的阿里云私有域名解析和管理服务，可以在自定义的一个或多个专有网络中快速构建 DNS 系统，实现私有域名映射到 IP 资源地址。

CDN：CDN 为全球用户提供一种可扩展、低成本、且适用于任何内容类型加速分发的内容分发服务，将源站内容分发至最接近用户的节点，使用户可就近取得所需内容，提高用户访问的响应速度和成功率。解决因分布、带宽、服务器性能带来的访问延迟问题，适用于站点加速、点播、直播等场景。

云企业网 CEN：云企业网（CEN）提供了一种混合的分布式全球网络，满足企业用户对网络覆盖的高需求。CEN 可以促进 VPC 与 VPC 之间以及 VPC 与 IDC 之间的通信。通过自动路由分发及学习，CEN 可以提高网络的快速收敛和网络的质量及安全性。

全站加速：全站加速构建于阿里云 CDN 平台之上，适用于动静混合型、纯动态型站点或应用的内容分发加速服务。全站加速 DCDN 通过动静分离、边缘缓存、智能路由、压缩传输等技术，解决跨运营商网络不稳定、单线源站、突发流量、网络拥塞等诸多因素导致的响应慢、丢包、服务不稳定的问题，提升动静态混合、纯动态站点/APP 的加速性能和访问体验。

弹性公网 IP：弹性公网 IP 将 ECS 和公用 IP 地址资源分离，支持可绑定到阿里云 VPC 型 ECS 实例、NAT 网关和 Intranet 负载均衡的独立公用 IP 地址资源。此外，它们可以动态解除绑定，从而将公共 IP 地址与 ECS 实例、NAT 网关和负载均衡器分离，满足灵活管理需求。

高速通道：高速通道是用于不同云网络环境之间的网络通信，包括连接多个 VPC 内部网络以及通过跨区域和用户的专线进行通信。

NAT 网关：NAT 网关是一款企业级的公网网关，提供代理服务（SNAT 和 DNAT），高达 10 Gbps 级别转发能力以及跨可用区的容灾能力。NAT 网关通过配置 SNAT 和 DNAT 帮助 VPC 建立互联网网关，从而更灵活地使用网络资源。

安全加速 SCDN：安全加速 SCDN 是一款便捷高效的网络服务，用于在云下和云上的不同网络环境间实现高速、稳定、安全的私网通信。安全加速 SCDN 使用物理专线连接实现云下 IDC 专线接入云上，提高网络拓扑灵活性和跨网通信质量；高速上云服务（ECC）基于阿里云智能接入网关的硬件能力和 SD-WAN 技术，为客户提供整合运营商物理专线的高可靠、高性能、低时延的一站式上云服务；对等连接实现云上跨地域/跨用户的 VPC 内网互通。

负载均衡（SLB）：负载均衡 SLB（Server Load Balancer）是一种对流量进行按需分发的服务，通过将流量分发到不同的后端服务器来扩展应用系统的吞吐能力，并且可以消除系统中的单点故障，提升应用系统的可用性。

专有网络 VPC：专有网络可帮助客户构建出一个隔离的网络环境。客户可以控制自己的专有网络、选择 IP 地址范围、设置不同的网段以及配置路由表和网关。

VPN 网关：VPN 网关是一款基于互联网，在阿里云 VPC 与企业数据中心、企业办公网络或互联网平台之间传输加密流量的服务，可用于建立可靠安全的数据传输连接。

安全

操作审计：操作审计通过收集云服务的 API 调用记录（包括控制台触发的 API 调用记录）进行安全分析、资源变更行为追踪和行为合规性审计等操作。它将操作记录规范化，并将其以文件形式保存到指定的 OSS 存储空间。

DDoS 防护：DDoS 防护服务是以阿里云覆盖全球的大流量清洗中心为基础，结合阿里巴巴自研的 DDoS 攻击检测和智能防护体系，向用户提供的可管理的 DDoS 防护服务，自动快速地缓解网络攻击对业务造成的延迟增加、访问受限，业务中断等影响，从而减少业务损失，提升安全防护等级，降低未知 DDoS 攻击风险。

运维安全中心（堡垒机）：运维安全中心（堡垒机）可以集中管理资产的运维权限、监控所有运维操作并实时还原运维场景，保障身份可验证、权限可管控、操作可审计。堡垒机可用于解决各种资产管理困难、职责权限不明确、运维事件回溯困难等问题。

配置审计：配置审计（Config）是云上 IT 系统治理服务。配置审计将为用户持续监控资源的变更，让用户了解资源配置随时间的演进。用户可以把企业的云上合规要求在配置审计设置为合规规则，配置审计将根据用户的设置自动为用户执行规则。当配置审计发现用户的资源配置不合规时，用户会收到相应告警。还将支持用户为不合规的情况设置手动或自动触发的修正程序。实现合规性的自主监管。配置审计将用户分散在各地域的资源整合为全局资源列表，用户可以便捷地查看全局资源。

云防火墙：阿里云云防火墙是业界首款公共云环境下的 SaaS 化防火墙。阿里云云防火墙可统一管理互联网到业务的访问控制策略，还可管控 VPC 之间，以及云企业网、高速通道之间，及 VPN 远程访问的流量。集中管理公网 IP 的访问策略，并且内置的威胁入侵检测模块（IPS）及主动外联检测，支持全网

流量可视和业务间访问关系可视，保存 6 个月网络流量日志，是用户业务上云的第一个网络安全基础设施。

漏洞扫描：漏洞扫描（CSS）利用数据、白帽渗透测试和机器学习为域和其他在线资产提供一站式安全解决方案。可检测网络漏洞、非法内容、网站篡改和后门程序，防止由于品牌声誉受损而造成的经济损失。

内容安全：通过深度学习提供多媒体内容风险的智能识别服务，阿里云 CSS 不仅可以帮助用户减少色情、暴力、恐怖主义及与政治相关的违规行为风险，还可以大大降低人工审核成本。

加密服务：加密服务通过使用经国家密码管理局检测认证的硬件密码机提供云数据加密和解密的解决方案。

数据库审计：智能解析数据库通信流量，细粒度审计数据库访问行为，通过对数据库全量行为的审计溯源、危险攻击的实时告警、风险语句的智能预警，为用户最敏感的数据库资产做好最安全的监控保障。

风险识别：风险识别是一种智能、轻巧、成熟的业务风险控制解决方案，可为企业用户快速缓解业务风险并减少损失。

应用身份服务：应用身份服务（IDaaS）是集中式身份管理服务，为政府和企业客户提供统一的应用门户、用户目录、单点登录、集中式授权和行为审核服务。支持通用的身份联合协议，还可以与其他身份源连接以实现统一的身份授权管理和应用访问控制。

密钥管理服务：阿里云密钥管理服务（KMS）是一项全托管服务，通过创建、删除和管理加密密钥保护用户数据。对于常见的密钥管理场景，用户可以使用 API 或阿里云管理控制台生成和管理客户主密钥（CMK）。

访问控制：访问控制（RAM）是一项管理用户身份与资源访问权限的服务。使用 RAM，用户可以集中管理 RAM 用户（包括员工，系统或应用程序），并可以安全控制这些 RAM 用户对资源的操作权限。

云安全中心：云安全中心是集成了 Server Guard 和威胁检测服务的旗舰安全产品。它是一个统一的安全管理系统，可实时识别、分析安全威胁并发出警报。借助安全功能，用户可执行自动化安全操作、响应和威胁跟踪，保护云和本地服务器的安全并满足法规合规性要求。

敏感数据保护：敏感数据保护（SDDP）可自动发现大量用户授权数据中的敏感数据，并对其使用进行检测、记录和分析。SDDP 检测安全合规违规行为并预测风险，帮助用户防止数据泄漏，满足一般数据保护法规要求。

Web 应用防火墙（WAF）：Web 应用防火墙（WAF）是一种云防火墙服务，可保护核心网站数据并维护客户网站的安全性和可用性。借助阿里云安全大数据能力，Web 应用防火墙可防止基于 Web 的攻击，包括 SQL 注入、XSS、恶意 BOT、命令执行漏洞和其他常见的 Web 攻击。

存储服务

块存储：块存储是为云服务器 ECS 提供的低时延、持久性、高可靠的数据块级存储产品。块存储支持在可用区内自动复制用户的数据，防止意外硬件故障导致的数据不可用，保护用户的业务免于组件故障的威胁。就像对待硬盘一样，用户可以对挂载到 ECS 实例上的块存储做分区、创建文件系统等操作，并对数据持久化存储。

文件存储 NAS：文件存储 NAS（ File Storage NAS）是一种分布式的网络文件存储，为 ECS、HPC、Docker、BatchCompute 等提供安全、无限容量、高性能、高可靠、简单易用的文件存储服务。

混合云备份服务：混合云备份 HBR（Hybrid Backup Recovery）作为阿里云统一灾备平台，是一种简单易用、敏捷高效、安全可靠的公共云数据管理服务，可以为阿里云 ECS 整机、ECS 数据库、文件系统、NAS、OSS 以及自建机房内的文件、数据库、虚拟机、大规模 NAS 等提供备份、容灾保护以及策略化归档管理。

日志服务：日志服务（Log Service，简称 LOG/原 SLS）是针对实时数据一站式服务，在阿里集团经历大量大数据场景锤炼而成。提供日志类数据采集、消费、投递及查询分析功能，全面提升海量日志处理/分析能力。

对象存储 OSS：对象存储 OSS 是一种完全托管的对象存储服务，可从任何地方存储和访问任意数量的数据。阿里云对象存储服务（OSS）提供行业领先的可扩展性、持久性和性能。所有规模和行业的客户都可以使用它来存储和保护任何数量的用例数据，例如备份和恢复、内容分发、数据湖、网站、移动应用程序、数据归档和物联网设备。

表格存储: 表格存储（Table Store）是构建在阿里云飞天分布式系统之上的分布式 NoSQL 数据存储服务。表格存储通过数据分片和负载均衡技术，实现数据规模与访问并发上的无缝扩展，提供海量结构化数据的存储和实时访问。

本报告所涵盖的数据中心区域

阿里云致力于提供稳定可靠的计算和数据处理能力，进而实现世界互联。阿里云拥有 75 个可用区，遍布全球从西到东 23 个区域。

本报告所涉数据中心范围覆盖以下地区：

- 中国·北京
- 中国·成都
- 中国·广州
- 中国·杭州
- 中国·河源
- 中国·呼和浩特

- 中国·青岛
- 中国·上海
- 中国·深圳
- 中国·乌兰察布
- 中国·张家口
- 中国·香港
- 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
- 美国·弗吉尼亚
- 马来西亚·吉隆坡
- 阿联酋·迪拜

注：有四个新的可用区在 2020 年 10 月 1 日至 2021 年 9 月 30 日期间设立。他们分别位于北京、广州、上海以及雅加达。这些可用区的检查期间为他们各自的设立日至 2021 年 9 月 30 日。

II. 控制环境、信息和沟通、风险评估、控制活动和监控活动概述

内部控制以及政策、程序、标准和工作指引由阿里云董事会、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——作为实施内部控制、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——确保员工能够通过信息和沟通体系获取和传达与需要实施的内部控制相关的信息，并且管理信息沟通活动的进行；
- 风险评估——识别并系统分析在运营活动中可能阻碍内部控制目标实现的相关风险，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以实现控制目标，并且确保该控制的有效运行。

本节概述简要描述了内部控制的前四个要素。控制活动将在下一节中介绍。使用一项或多项阿里云服务以支持其财务报告流程相关关键系统的阿里云客户可借助本报告了解阿里云控制的设计和运行。

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。阿里云利用了集团层面控制环境的某些方面。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，在内部制定了各类政策、程序和标准并进行了妥善传达。

阿里云由阿里云首席执行官领导，其直接向集团首席执行官汇报。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。每个部门的汇报关系和部门内相应人员的相关信息均通过集团信息门户网站向全体内部员工开放，以确保良好的运行效率和明确的职责分离。

阿里云安全事业部负责构建云安全防护生态系统，设计、开发和运营云安全产品，以及执行云安全性和合规性管理。阿里云安全事业部负责人同时担任阿里云首席信息安全官，负责云安全生态系统、云安全管理和合规性相关事宜。安全事业部的行业合规和标准团队负责管理与云计算相关的外部标准合规性、与外部监管机构进行沟通、构建信息安全管理体系和内部检查程序和建立风险识别和评估流程，并定期开展风险评估。安全事业部的云安全团队负责云产品和系统的安全管理，并定义了安全标准和云安全运维基准。

阿里云遵循集团的员工招聘、入职和培训计划。人力资源部会对符合特定条件的潜在员工进行背景调查。按照潜在员工的不同级别开展具体的背景调查（如工作经验和商业利益）。所有新员工都必须签署保密协议。所有新员工都必须参加有关公司文化、愿景、核心价值观、道德、行为准则和个人职业发展的培训。在专业培训中，各团队将通过在线学习平台分享技能；员工还可参加由内部和外部资深专家举办的线下培训和交流会。高级主管可通过专门的管理培训计划来扩展管理视野和思维。全体在职员工每年都必须完成信息和数据安全性在线培训和评估。

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。

新政策和相关更新均通过内部门户网站传达。根据已制定的相应政策和治理标准，所有部门均须按照标准要求制定和发布政策。

阿里云制定了针对云服务的服务水平协议（SLA），其中包括各项性能指标和赔偿条款。客户可通过阿里云官网获取该 SLA。阿里云在阿里云控制台中提供了工单服务，以支持客户向阿里云报告与安全性、可用性和保密性相关的故障、事件、疑虑和投诉。对于提供给客户的每一项阿里云服务，均由一名指定产品经理负责相关的市场开发和客户需求调研。优先客户均配备专门的客户经理负责沟通。客户可以通过热线电话、阿里云控制台、钉钉即时消息工具等报告问题。相应的阿里云工作人员（例如相应的客户经理、售后人员、技术支持和云服务团队）将跟进报告的问题，并及时向客户提供反馈。

公共沟通由阿里云品牌和公共传播事业部的公共关系团队负责。如果发生影响客户或阿里云声誉的事件，将由公共关系团队在完成内部审核和审批后进行外部沟通。此外，阿里云构建的沟通流程可通过阿里云控制台、电子邮件、短信和钉钉将可能对客户造成影响的事件通知客户。

阿里云组建了专业培训团队，可为客户提供培训和支持，以帮助其有效使用云服务。

3. 风险评估

阿里云构建了风险管理框架，以识别、分析和管理与公司内部以及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。

阿里云根据潜在影响和发生的可能性对变更进行风险评级。阿里云针对不同风险等级的变更制定了相应的变更流程，以确保为高风险等级变更提供更多资源和控制措施。

阿里云基础设施事业部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。风险管理人员定期开展风险评估和应急演练测试，并要求相关供应商针对可能影响运行的风险制定改进计划。

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。

此外，阿里云还每年聘请独立外部审计师进行外部审计，例如 ISO 认证。此类外部审计每年计划和执行一次，旨在测试阿里云实施的控制的设计合理性和运行有效性。

每次审计完成后，审计师将审计报告提交至管理层，由管理层负责制定和执行相应的纠正计划。管理层会定期跟踪和监控纠正计划和措施。

III. 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， 旨在有效实现阿里云的控制目标。阿里云的内部控制要素包括对整个组织具有广泛影响或与特定流程和应用程序相关的控制。

1. 信息安全治理与风险管理

阿里云为包含流程和系统在内的信息安全管理推行了信息安全策略。信息安全策略总体上涵盖风险管理、安全战略、信息安全组织、资产管理、人力资源管理、物理和环境安全、通信和运行管理、访问控制、信息系统采购、开发和维护等。信息安全管理体系的管理程序包括信息安全管理体系的建立、内部审核、管理评审、绩效评估和持续改进.

阿里云明确了信息安全组织架构内部成员和各业务部门（包括信息管理指导委员会、信息内部审计工作组、信息安全工作组、云安全合规团队、云平台安全团队及阿里云各项服务安全接口人）的职责。各部门安全接口人负责执行章程明确的信息安全机制，包括监控日常工作中的安全事件、协调信息安全意识培训、协调资源以支持信息管理内部审计和风险评估以及其他相关的信息安全培训；

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。

阿里云制定了《信息安全风险评估管理规定》,旨在规范信息安全风险识别和评估程序、风险分类方式、风险承受能力定义、解决超出承受能力风险的程序、风险评估频率和风险评估涵盖的领域。阿里云每年至少开展一次信息安全风险评估，其涵盖风险概率和影响分析，并且会根据评估结果更新安全政策。同时，会对政策版本更新信息进行跟踪记录。

信息管理指导委员会每月组织业务部门和风险及合规部门的领导讨论业务更新、政策更新、技术环境变化及其影响。

2. 人力资源

阿里云制定了《人力资源安全管理规定》，旨在规范招聘、录用和职责划分流程的安全要求，以及违反安全政策的惩戒措施、违规行为的分类标准和相应的处罚规定。同时，该管理规定要求员工参加安全意识培训了解公司的信息安全管理政策，承担和履行岗位相关的信息安全责任。

阿里巴巴集团制定了《商业行为守则》，以明确员工的责任，规范员工遵守既定政策和程序及适用的法律、法规或监管合规的义务。管理层根据需要对《商业行为守则》进行审查和更新。员工必须每年完成一次《职业道德和行为守则》在线测试。

根据《阿里云人力资源安全管理规定》的要求，新入职员工需接受背景调查、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。阿里云设计并实施了标准的员工离职流程，确保离职时完成返还公司资产、终止访问权限等必要程序。同时，及时在人力资源系统内更新员工状态，以触发终止访问权限的程序。相应的人力资源团队负责确保员工离职程序相关控制有效运行。

阿里云与员工之间保密协议中的法律规定由法务部每年至少进行一次审核和更新。

阿里云制定了培训方案，对员工进行适用政策、标准和信息安全实践方面的培训，并持续对员工进行信息安全培训。作为入职流程的一部分，员工在完成安全意识培训后，必须通过数据安全测试。

阿里云每 6 个月开展一次员工绩效评估，评估内容包括业务表现以及员工行为是否符合公司核心价值观。此外，阿里云成立了独立的阿里云数据安全团队，开通了多个上报渠道，以监督和识别员工违规行为。任何违反信息安全政策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。

请参阅“供应商管理”一节获取更多有关供应商和第三方员工的人力资源管理细节。

3. 数据安全管理

阿里云数据安全管理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。

阿里巴巴制定了《阿里巴巴集团数据安全规范》，旨在定义不同的数据类型（即客户数据、业务数据和公司数据）、数据所有者、数据分类标准、数据安全等级、数据保护措施以及数据安全管理生命周期。数据安全生命周期的每个阶段都有其相关的安全管理要求和技术。阿里云遵循集团的政策和要求，以确保由阿里云管理的数据的安全性。

数据保密性

阿里云在服务协议中定义了客户和阿里云各自的责任和义务，协议中包括阿里云提供的服务类型 和等级以及关于保密性和数据披露的条款。客户在使用相关产品服务之前需要确认并同意服务协议。另外，阿里云通过其官网与客户沟通最新的保密政策，并以合同条款的形式向供应商和其他第三方传达最新的保密政策。

阿里云运维人员在未获得客户事先同意和授权的情况下，没有权限访问客户未披露的数据。此外，阿里云遵循生产数据不出生产集群的原则，从技术上阻断生产数据流出生产集群的通道，从而防止运维人员从生产系统中拷贝数据。

数据采集和分类

阿里云制定了数据分类及安全等级规范，以定义数据分类标准和数据安全级别。阿里云建立了一个数据安全平台对数据信息进行更新和维护，包括数据的保留时间、分类和安全级别等信息。修改数据的分类分级需要遵循严格的审批流程。

数据采集安全要求数据的识别、分类和分级在数据创建和采集的第一时间完成，以确保后续对云数据采用恰当的安全保护机制。其中，首先对数据中的敏感信息进行发现和检测，其次根据用户的使用场景、合规需求、和安全要求对数据中的敏感信息进行分类分级，并在后续对数据进行针对性的保护。

数据加密

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、以及硬件内存加密。在适用的情况下，数据在备份前和传输中都会进行加密处理。更多详情请参见“加密和密钥管理”一节。

数据备份

阿里云实施了一系列针对关键系统组件的备份流程。阿里云关键系统组件必须每周全量备份至少两次，备份时间和频率由各团队决定。阿里云对关键系统组件采用多可用区备份机制。阿里云对关键系统组件的备份进行加密。阿里云关键系统组件的备份由系统监控，如果出现备份错误或故障，系统会自动触发全量备份，直到备份成功为止。此外，阿里云还建立了备份恢复和检查的自动程序，每个月对关键系统组件的备份进行恢复，并对恢复的数据进行完整性检查。

数据冗余和复制

阿里云采用冗余机制和故障自动迁移恢复来保障用于支持客户服务的关键系统组件的高可用性。这种自动对故障进行检测并且对系统进行保护性迁移的设计，可以最大限度地减少对客户服务的中断。另外，阿里云采用多可用区机制，将关键系统组件分散存放在多个可用区。

另一方面，针对客户的数据，阿里云通过分布式存储实现多副本数据冗余，以提高客户数据的可用性。分布式存储机制将文件分割成多个数据片段存储在不同的设备上，并且每个数据片段存储多个副本。

OSS 采用多可用区冗余储存机制，将用户的数据分散存放在同一地域的 3 个可用区。当某个可用区不可用时，仍然能够保障数据的正常访问。

此外，云数据库 RDS 版支持多可用区实例，也称为同城容灾实例。多可用区实例将物理服务器部署在不同的可用区，当一个可用区出现故障时，系统会立刻将工作负载切换到另一可用区。整个切换过程对用户而言是透明的，无需更改应用程序代码。通过使用数据传输服务，云数据库 RDS 版也可支持跨区域的数据容灾。此外，客户还可利用阿里云基础设施的地理分布特性，实现高可用性架构并提供故障热迁移能力。

数据销毁

阿里云建立了对设备全生命周期（包含接收、保存、安置、维护、转移以及重用或报废）的安全管理。阿里云严格管理设备的访问控制和运行状况监控，并且定期进行设备维护和盘点。对回收或停运的设备，

阿里云建立了相应的存储介质数据安全擦除流程。在处置数据资产前，阿里云检查含有数据的媒介是否经物理销毁，以确保数据无法恢复。在对任何设备进行回收或将设备从数据中心迁移出去之前，阿里云会进行多次覆盖数据的操作，且确保系统会记录这些擦除数据的操作。当因业务或法律原因不再需要某些实体材料时，阿里云对其进行物理销毁，或从第三方数据处理机构处获取销毁证明，以确保数据无法重建。

客户数据的擦除和处理

数据擦除是存储虚拟化的延伸。当释放云用户实例服务器后，其原有的磁盘和内存空间将会被可靠地进行数据清除，以确保用户数据安全。

阿里云在终止向云服务客户提供服务时，会使用符合行业标准的数据擦除技术及时删除客户的数据资产，或根据相关协议将数据资产归还给客户。同时，阿里云也会对数据擦除操作进行记录，以防止客户数据被未授权访问。

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。

网络隔离

阿里云将生产网络与非生产网络进行隔离，从非生产网络无法直接访问生产网络中的任何服务器和网络设备。阿里云在生产网络边界上部署了堡垒机，办公网内的运维人员只能通过堡垒机访问生产网进行运维管理。运维人员登录堡垒机时，需要使用动态口令以及域账号和密码进行双因素认证。堡垒机使用加密算法以确保运维通道数据传输的保密性和完整性。

另外，阿里云将对外提供服务的云服务网络与支持云服务的物理网络进行安全隔离，通过配置网络 ACL 确保云服务网络无法访问物理网络。阿里云还采取网络控制措施以防止未授权设备连接到云平台的内部网络，并防止云平台的物理服务器连接外部设备。

租户隔离

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。该机制防止未授权访问租户间的系统资源，并确保计算节点间的基本计算隔离。同时，虚拟化管理层还提供存储隔离和网络隔离。

- 计算隔离

阿里云提供多种基于云的计算实例和服务，能够自动伸缩以满足应用或业务需求。这些计算实例和服务提供多级别的计算隔离以保护数据，并同时确保用户需求的配置灵活性。计算隔离中关键的隔离边界是管理系统和客户虚拟机之间的隔离，以及客户虚拟机之间的隔离，这种隔离由 Hypervisor 直接提供。阿里云平台使用的虚拟化环境将用户 ECS 实例作为独立虚拟机运行，通过使用物理处理器不同权限级别强制执行隔离，以避免用户的虚拟机在未授权的情况下访问物理主机和其他用户虚拟机的系统资源。

- 存储隔离

在云计算虚拟化的基本设计中，阿里云将基于虚拟机的计算与存储分离。这种分离使得计算和存储可以独立扩展，让提供多租户服务变得更简单。在虚拟化层，Hypervisor 使用分离设备驱动模型进行 I/O 虚拟化。虚拟机的所有 I/O 操作都会被 Hypervisor 截获处理，以确保虚拟机只能访问分配给其的物理磁盘空间，从而实现不同虚拟机之间硬盘空间的安全隔离。

- 网络隔离

为了向 ECS 虚拟机提供网络连接，阿里云将虚拟机连接到阿里云虚拟网络。阿里云虚拟网络是构建在物理网络结构之上的逻辑结构。所有逻辑虚拟网络之间都相互隔离。这种隔离可以防止网络流量数据被其他恶意实例监听或拦截。

此外，阿里云定义了安全组，以控制对 ECS 实例的访问。不同安全组中的 ECS 实例默认无法相互访问。可以通过配置安全组规则来控制对 ECS 实例的网络访问权限。

操作系统和镜像加固

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相关标准进行配置。

阿里云 ECS 租户可使用镜像创建 ECS 实例或更改 ECS 实例的系统盘。客户可从云市场上选择镜像或使用自己的自定义镜像。阿里云公共镜像的安全加固包含三部分：镜像基础安全配置、镜像漏洞修复和镜像中的默认安全软件。此外，所有阿里云公共镜像都默认包含阿里云安全软件（例如安全中心），以确保实例在启动时的安全性。在宿主机部署 ECS 实例时可能会由于性能异常或硬件原因产生故障。当检测到宿主机故障时，系统将启动保护性迁移，将 ECS 实例从发生故障的宿主机自动迁移到正常的宿主机上，以确保应用的可用性。

阿里云实时监控阿里云公共镜像操作系统和第三方软件里的漏洞，以确保阿里云公共镜像里的高风险漏洞及时得到修复。检测到新的高风险漏洞后，阿里云镜像会通过更新来集成已知的高危漏洞补丁，防止主机上线后处于高风险状态。有关漏洞管理流程的详细信息，请参见“威胁和漏洞管理”一节。

虚拟机镜像的更改必须在变更管理系统上进行申请并且通过预定义的审批工作流。验证方法和测试结果也应当记录在变更系统中。阿里云通过官网与租户客户沟通已发布的变更。虚拟机镜像的更改流程遵循“变更管理”一节所述的相同流程。

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，以确保阿里云环境中资源和系统的访问得到适当的管理和限制，进而防止信息资产受到未授权访问。

用户账号管理

阿里云使用集团账号管理平台对访问阿里云环境中的系统和资源的账号进行集中管理，仅允许单点登录。每个员工的 Active Directory （AD） 账号都是唯一的，可对应到唯一使用人，并且不得共享的。账号管理平台利用从人力资源管理系统中自动同步的员工信息进行账号管理。当新员工入职信息录入到人力资源管理系统时，账号管理平台会自动为新员工创建新 AD 账号；员工在岗的最后一天，根据来自人力资源系统的自动数据传入，账号管理平台会自动停用该离职员工的 AD 账号。

权限和访问管理

阿里云基于业务需求分配权限，并根据用户的具体角色、职责以及其负责的具体事务授予能完成其工作的最小资源访问权限。阿里云使用权限管理系统集中管理用户权限的申请、审批、权限的自动分配或移除。

员工通过权限管理系统根据需要申请访问权限。根据相关的风险等级权限被划分为不同的级别，权限申请的审批机制也根据其对应的不同的级别有所不同。授权人员一旦批准了申请，相应的权限将自动授给提出申请的员工。权限管理系统中实施了职责分离控制，要求所有权限申请至少获得用户主管的批准，且申请人与审批人不得为同一人。

网络设备和服务器的访问权限根据风险等级分为三种类型，即一般用户、应用管理员和系统管理员。权限管理系统根据权限类型预先设置了对应的审批工作流，并根据相应系统中存储的系统负责人信息和应用负责人信息确定工作流审批人。Root 账户不开放给用户在权限管理系统中申请并且 Root 账户的密码每个月会定期轮换一次。Root 敏感权限只分配给授权用户。Sudo to root 的操作也在日志管理平台上被记录并且监控。

权限管理系统利用从人力资源管理系统自动同步的员工信息，以在用户离职、转岗或工作职责发生变化时对用户的访问权限进行管理。 对于离职的用户，系统会自动回收该用户的所有权限。对于职责发生变更或调岗至不同部门的用户，系统会自动向用户的主管发送通知以便主管审核用户的访问权限，并根据当前工作职责回收任何不再需要的访问权限。

密码控制

阿里云制定并实施了账号密码策略（包括密码长度、密码复杂度、密码使用期限、密码历史、最多登录尝试次数和初始密码更改），并要求用户设置符合策略要求的密码。

远程访问

员工必须使用域账号和密码加上注册设备上接收到的动态验证码完成双因素认证，才能通过 VPN 从公网访问阿里云内网。

权限审核及监控

权限监控系统内定义了审核及监控规则，以分析账户和访问权限的使用情况，进而检测潜在的权限滥用情况，并在发现任何偏差或异常情况时自动发出警报并通知安全团队。安全团队负责追踪警报情况并采取适当行动。

记录和监控

员工对生产系统的所有运维操作只能通过堡垒机进行。所有操作过程会被完整记录并实时传输到日志集中管理平台。员工在生产系统及其支持性的基础设施上执行的敏感操作也会通过日志的方式记录下来，这些日志也会传输到日志集中管理平台。日志集中管理平台上的信息受到保护，以确保未经授权无法进行访问日志且员工无法对日志修改或删除操作。

阿里云在日志集中管理平台定义了审核和监控规则，以监控敏感活动和检测异常用户活动。出现异常用户活动时，平台会自动发出警报并生成警报单，以便安全团队进行审查和跟进。

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。

阿里云制定了《信息资产安全管理规定》，以规范信息资产的识别、分类和管理。阿里云使用配置管理数据库以整合和维护云服务相关信息资产上不同系统的信息。基础设施数据团队负责管理和维护数据库。每项信息资产在数据库中都有详细记录和对应的资产负责人。相关团队根据需要对信息资产的标识和分类进行更新，确保资产信息是准确、完整、一致和最新的。配置管理数据库中所有资产信息的变更都会通过系统日志记录下来。

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恰当人员的授权。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。

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服务协议，其中定义了客户和阿里云在客户访问权限管理方面各自承担的责任和义务，同时包括保密性条款和保密协议。在阿里云账号注册或产品购买流程中，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一个唯一的阿里云账号。客户进行自助密码重置前，需要通过经验证的手机上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访问阿里云客户的资源，都必须经过客户授权和身份验证。此类临时访问请求及相关审批通过阿里云管理控制台的工单服务进行管理。

8. 加密和密钥管理

阿里云采用最先进的加密技术以有效地加密和管理密钥，进而确保敏感数据的保密性、真实性和完整性。

阿里巴巴集团的《数据安全规范》要求必须对敏感数据采取包括加密在内的保护措施。阿里云制定了《阿里云密码和密钥管理规定》对密钥生命周期（包括密钥的生成、存储、使用、分发、备份、更换和回收）进行管理。该规定也涵盖了标准加密算法、密钥管理和职责分离的规范和要求。

密钥管理服务 （KMS） 是由阿里云提供的安全管理服务，旨在提供密钥的安全托管、密码运算等功能，并执行安全措施如密钥轮换。KMS 同时兼容其他云产品并支持对其他云产品管理的用户数据进行加密保护。KMS 的认证和访问许可由阿里云 RAM 服务进行控制和管理。

阿里云提供了全链路的加密保护（包括传输加密、存储加密，以及基于硬件的加密计算环境）以保障数据安全。同时，阿里云提供了基于硬件加密机 （HSM） 的加密服务，为用户提供一整套数据加密的解决方案。阿里云的密钥管理基础设施遵循 （NIST） 800-57 中的建议，并按照相关的合规要求使用了加密算法和 HSM 。阿里云密钥管理服务使用的 HSM 已通过了国际和国内双重认证。中国大陆以外地区使用的 HSM 获得了美国 FIPS 140-2 三级认证。

加密计算

阿里云利用阿里云加密计算技术为可信执行环境中的用户数据提供数据加密。阿里云平台使用 Intel Soft Software Guard Extension （Intel SGX）来提供硬件可信的执行环境。基于此，用户可建立可信的执行环境来保护其敏感数据，例如加密/解密密钥和账户凭证信息。用户可通过编写支持可信执行环境的代码来保护数据，以确保客户的关键数据仅能通过其编写的代码进行访问和操作。所有的加密信息只能在可信执行环境中计算和运行，从而提供基于硬件的数据保护。

传输加密

阿里云制定了《阿里云信息传输安全管理规定》，明确数据传输的安全管理要求和措施。阿里云产品使用了传输层安全 （TLS） 协议来确保为用户读取和上传数据时数据传输的安全。阿里云控制台使用超文本传输安全协议 （HTTPS） 进行数据传输。阿里云产品为用户提供了支持 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的需求。

阿里云的网关产品也提供传输链路的加密功能。VPN 网关服务可通过传输链路加密通道将企业本地 IDC 和阿里云 VPC 安全可靠地连接起来。VPN 网关可建立 IPsec-VPN 连接，将本地 IDC 网络和云上 VPC 连接起来。也可建立 SSL-VPN 连接，将本地客户端远程接入 VPC。

静态加密

通过阿里云密钥管理服务的密钥，阿里云支持客户对储存在服务环境中的静态数据进行加密。阿里云的存储加密提供 256 位密钥的存储加密强度，满足敏感数据的加密存储需求。

基于产品特性和客户需求，阿里云不同产品的存储加密设计略有不同。总体而言，存储加密中至少包括两层密钥，第一层为客户主密钥（CMK），第二层为数据密钥（DEK）。其中 CMK 用来为 DEK 进行加解密操作和保护，DEK 用来为真实数据进行加解密操作和保护。云产品的静态加密功能支持使用托管给云产品的服务密钥作为主密钥。阿里云也有多个产品支持用户自选密钥功能，包括用户自上传的 CMK 或用户自己在 KMS 中生成的用户主密钥都可用作 CMK 对数据进行加密。用户自选的 CMK 是用户的资产，云产品必须通过 RAM 得到用户的授权后才可以使用其对数据进行加解密操作。

阿里云有不同的云产品支持数据存储加密功能。其中，OSS 支持服务器端和客户端的存储和加密。在服务器端的加密中，OSS 支持使用服务密钥和用户自选密钥作为 CMK 进行数据加密。在客户端的加密中，OSS 支持用户使用用户自管理密钥或用户 KMS 内的 CMK 进行客户端的加密。另外，RDS 数据库的多个版本提供透明数据加密或云盘实例加密机制，并支持使用服务密钥和用户自选密钥作为 CMK 进行数据加密。NAS 文件存储和 MaxCompute 也支持使用服务密钥作为 CMK 来进行数据加密。

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。

访问管理

数据中心设立并分隔了服务器机房区、办公区以及运输区来进行权限安全管理。服务器机房区用于存储信息技术设备和信息系统，该区域得到保护以防止未经授权的访问。办公区用于数据中心现场人员的工作场所。运输区设置在服务器机房外，用于运输和交付设备。

阿里云各数据中心都配备了门禁卡系统用于管理访问权限。只有获得授权的阿里云员工和数据中心服务商的工作人员可以使用该门禁卡系统。数据中心实施了读卡器、生物特征识别机制、或物理锁等物理访问机制来限制对数据中心服务器机房的访问。

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。其他人员若因业务需要要进入数据中心，必须提前提交申请，经相关数据中心经理审批后才能获得临时访问权限。数据中心经理须将该其他人员的身份告知数据中心服务商在数据中心的运维人员。该其他人员每次出入数据中心时都必须出示个人证件并进行登记，且访问期间需由数据中心运维人员全程陪同。

每个月适当的人员会对数据中心的访问权限进行审核，以确保用户访问权限的适当性。

环境控制

阿里云各数据中心配有使用热传感器和烟雾传感器的火警检测系统，传感器安装于天花板和地板下面，触发时会发出声光报警。数据中心也配有集成气体灭火系统和手动灭火器。另外，数据中心人员定期进行火灾探测和响应的培训和演练。

阿里云数据中心采用精密空调来保障恒温恒湿的环境。所有空调机组均采用热备冗余模式。阿里云数据中心配置了传感器来监测与控制温度与湿度。

阿里云在数据中心、设备交付区和所有关键访问点的出入口处都安装有视频监控设备，且监控视频记录至少保存三个月。

为保障阿里云业务 7*24 小时持续运行，阿里云数据中心采用双路电源和冗余电力系统供电。主备电源及系统具备相同的供电能力。当电源出现故障时，冗余电池组和柴油发电机会为数据中心设备进行供电，保障数据中心在一段时间内的持续运作能力。

监控控制

阿里云数据中心现场人员负责监控数据中心的物理监控措施，包括机房的暖通空调 （HVAC） 、避雷系统、火灾探测和灭火系统、电源系统、用来监测温度与湿度的传感器等。

阿里云数据中心驻场人员轮流监控数据中心的运行。数据中心环境（如温度、湿度等）和服务器性能由设备监控系统进行实时监控。如有异常，系统会自动触发警报，驻场人员会与数据中心服务商对接以解决问题。

10. 终端安全

阿里云设置了相关的要求和程序以管理移动设备，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。

阿里云在员工的计算机（包括公司提供的以及员工自带的）上部署了终端管理系统。只有在安装和启动了该系统之后，计算机才能连接到阿里云的 OA 子网，以进行网络准入和终端保护。该终端管理系统同时被用于控制计算机上的软件安装，并在系统内列出了所有授权安装的软件。

所有计算机在发放给员工前会完成标准镜像的安装。该标准镜像中包含了防病毒软件以及硬盘加密软件，且员工无法卸载这类软件。 员工无法关闭防病毒软件的功能，并且需要输入由 IT 部门集中管理的密码才能卸载防病毒软件。

员工的计算机上安装有数据泄露防护 (DLP) 软件，用于监控文件传输和检测在计算机上执行的敏感操作。计算机上的终端管理系统监控 DLP 软件的安装状况，如发现计算机未配备 DLP 软件，系统将自动将 DLP 软件推送到计算机上安装。

阿里云设置了专门的监控系统，按照预定义的审核规则对 DLP 软件中收集到的活动进行分析，并自动生成潜在数据泄漏警报以供安全团队跟踪并采取适当的行动。

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。阿里云制定《安全事件、漏洞应急处理体系》，以规范安全漏洞的管理，包括安全漏洞的分类和响应机制。

阿里云通过多个渠道收集和发现安全事件和漏洞，包括来自内部和外部的上报、内部漏洞扫描和外部漏洞发布平台的订阅。外部上报的渠道包括阿里巴巴应急响应中心、阿里云先知漏洞平台、外部报告的开源第三方组件通用漏洞披露信息（CVE）以及来自第三方的威胁情报信息。

阿里云建立了安全事件和漏洞管理平台以集中管理上述渠道收集的安全事件和漏洞。安全团队每天审核平台上的事件和漏洞，对上报的漏洞和安全事件的真实性进行排查确认。一旦确认为安全事件和漏洞，安全团队会启动应急响应流程并指派相应的人员负责解决问题。应急响应团会评估安全事件和漏洞、确定其安全等级和优先级，并安排解决方案。同时，安全团队也会及时通过线上公告的方式第一时间通知用户。

安全团队设立了安全配置的基线标准，其中明确了操作系统、数据库管理系统、网络设备和虚拟镜像的基线要求。安全部门至少每年进行一次基线标准的检查和更新。另外，阿里云部署了扫描工具对操作系统、数据库管理系统、网络设备和虚拟镜像的配置进行扫描和分析。分析结果将自动汇集到安全事件和漏洞管理平台。当检测结果与基线标准存在差异时，相关运维人员会将其恢复到标准水平。检测和恢复结果会汇总到周报中做进一步的跟进。

阿里云的服务器上安装有入侵检测软件，用于检测潜在的入侵行为。另外，阿里云还设立了网络监控系统用于实时监控网络流量和用户操作，并识别异常操作。安全团队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。

阿里云实施了云平台侧的攻击和防御对抗演练计划。阿里云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，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，并将发现的漏洞记录下来进行分析。

12. 安全事件管理

阿里云的安全事件管理流程通过监控和检测安全事件并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。

阿里云对云平台安全性进行监控以发现攻击平台资源的安全事件，并触发安全事件响应流程以恰当处理事件。记录员工在云平台上操作的日志会被分别导入实时和离线计算平台。并通过每个计算平台中的安全监视算法对日志进行处理和分析，以识别和检测异常操作。

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。安全团队审核安全事件监控平台上的分析结果，对事件进行排查并确认是否为安全事件。根据安全事件的严重性和安全级别，安全团队会将发现的安全事件通知和上报给相应的团队，以便及时采取后续跟进行动。

阿里云通过阿里云官方网站、短讯、邮件或钉钉信息发布可能影响客户的安全事件。

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，故障响应要求，以及不同风险等级故障的上报和解决流程，以确保及时地识别、评估、上报和解决故障。

阿里云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。全球运行中心（GOC）团队根据已建立的故障管理标准和应急响应程序负责管理故障使其得到解决。GOC 与产品团队合作确定需要在故障管理平台上监控的关键系统和事件。当故障管理平台发出警报时，GOC 首先确认警报是否与故障有关。一旦 GOC 在平台上确认故障，平台将自动向受影响的团队发送电子邮件通知并发起工单以便相应的团队进行跟踪解决。除了依赖故障管理平台的自动识别功能以外，GOC 团队还通过客服接收客户反馈并创建相应工单以收集故障案例，并采取相应解决措施。

安全团队每月组织一次内部会议，对上个月发生的故障进行根因分析，并与阿里云的业务领导层和项目经理讨论故障的后续跟进状况以及改善措施。

阿里云建立了多个渠道与客户沟通可能会对客户产生潜在影响的故障，包括阿里云官网公告、站内信、短信、电子邮件或钉钉消息。

14. 变更管理

变更管理流程

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被记录、评估、测试、审批以及在必要时进行沟通。阿里云成立了一个独立团队，监督变更管理的过程，监控变更管理政策和程序的合规情况，并调查由未经有效控制的变更引起的安全事故或故障。

所有会影响业务运行的变更，包括对系统元数据、软件、配置、基础设施、硬件和网络的变更，在适用的情况下都需要经历申请、测试、评估、审批、实施及复核等一系列阶段。阿里云采用 DevOps 开发模式来自动化和优化变更管理流程，从而以更快的速度提供持续性的服务。变更流程的各阶段都通过变更管理系统进行集中的跟踪记录，各阶段相关的支持文件也保留在变更管理系统中。

阿里云根据变更紧急程度以及潜在系统故障的影响进行变更等级划分，并根据变更来源和对象进行分类管理。根据变更发布时间，变更分为普通变更和紧急变更两类。普通变更在预定义的变更窗口发布，而紧急变更一般在变更窗口以外或封网期发布。

在提交审批之前，需对变更进行测试并记录相关测试结果。源代码变更需进行代码审核并记录审核结果。需针对变更制定并记录相关回滚方案，以支持操作人员在需要时撤销变更并恢复系统至之前的状态。

将变更部署于生产环境前，需在变更管理系统中提交变更请求，说明变更类型、风险级别、风险描述、变更原因、变更计划、回滚方案和验证方法。所有变更在部署到生产环境前都需要得到授权人员的审批。

在变更部署阶段，应记录变更方案、变更计划、变更评估和变更实施等。针对大规模变更，阿里云采用灰度发布流程，以分阶段推出经过测试和批准的变更，将变更逐步部署到生产环境中。在灰度发布期间，产品团队会密切监控变更部署状态并在必要时执行回滚程序。

在部署完成后，相关人员应对变更进行验证,对配置项进行复核，以及告知变更结果。此外，在适用情况下，阿里云会向可能受到变更影响的客户发送变更通知。

安全产品生命周期 (SPLC)

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，进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。

在产品立项阶段，安全架构师和产品方一同根据业务内容、业务流程、技术框架建立功能需求文档（FRD）、绘制详细架构图，并在确认适用于产品的安全基线要求。同时，本阶段会安排针对性的安全培训课程与考试给产品方人员，从而避免在后续产品开发中出现的安全风险。

在安全架构审核阶段，安全架构师在上一阶段产出的 FRD 和架构图基础上对产品进行针对性的安全架构评估并建立产品的威胁模型。随后，安全架构师会综合安全基线要求以及威胁模型分析中提出的安全解决建议方案，与产品团队合作确定产品的所有安全要求。

在安全开发阶段，产品团队会根据阿里云的安全编码规范和安全要求开发产品，并实现产品相关的安全功能和要求。为确保快速持续的开发、发布和部署，产品团队在该阶段会进行自评以确认安全要求都已经实现，并提供相应的测试信息（例如代码实现地址和测试报告），从而为下一阶段的安全测试审核做准备。

在安全测试审核阶段，安全工程师会根据产品的安全要求对产品的架构、设计和服务器环境实施全方位的安全复核，并在适用情况下对产品的代码进行代码审核和渗透测试。 在产品发布前，通过对代码扫描确认是否存在恶意软件。产品团队必须对该阶段发现的任何安全问题的进行安全修复和加固。

在应用发布阶段，只有在通过安全复核并获得安全审批许可后，才可通过标准发布系统把产品部署到生产环境。

在应急响应阶段，安全应急团队持续监控云平台以发现可能存在的安全问题，并通过内外渠道和安全自测来识别安全漏洞。关于阿里云的应急响应流程的详情，请参见"威胁和漏洞管理"一节。

环境分离和职责分离

阿里云就变更管理流程实施了相应的访问控制，以确保生产系统的访问权限遵循最小授权和职责分离的原则。阿里云部署了独立分离的开发、测试和生产环境，并严格控制不同环境的访问权限。同时，阿里云在变更管理流程中实施职责分离，确保变更的申请、审批和实施过程都有合理的职责分离控制，且只有经过测试和审批的变更才能投放到生产环境中。

源代码管理

阿里云建立了内部源代码库，用于控制和管理源代码的变更，并确保阿里云产品代码的高级别安全性。

阿里云的源代码库用于存储源代码并记录开发期间的源代码更改，以实现版本管理。依赖代码库的授权管理功能，每个团队可以根据最小授权原则有效地管理源代码的访问权限。在云产品安全生命周期中，阿里云安全专家严格审核和验证源代码的安全性。另外，阿里云持续对阿里云市场上的软件进行代码安全性扫描，以有效管理安全风险。

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，以确保在业务中断发生时及时恢复关键业务的运行。阿里云构建了业务连续性管理框架，其中包括业务影响分析、风险评估，以及《应急响应计划》和《业务连续性计划》的维护、实施、测试和持续改进。

业务连续性管理团队每年进行业务影响分析和风险评估，识别和记录可能导致阿里云关键业务运营中断的威胁，并针对不同的中断场景制定相应的策略。

阿里云制定了《业务连续性计划》，以指导在业务中断情况下或由意外、恶意或环境事件引起灾难的情况下进行业务恢复。《业务连续性计划》须每年审查一次，并在必要时进行更新。另外，阿里云制定了《阿里云应急响应计划》，以确定应急响应中的紧急情况分类、角色和职责、工作流程和资源管理要求。同时，阿里云也制定了事件响应计划，以响应与关键运营和服务、网络和 IDC 基础设施有关的事件。阿里云每年都会根据相应的业务连续性计划对阿里云关键产品进行业务连续性演练。另外，阿里云每年会在业务中断情况下对数据中心关键流程的持续运营和必要资源的业务连续性进行测试。

阿里云遵循既定程序进行需求预测、容量监控和计划，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带来的资源可用性风险。阿里云实时监控容量，并在预测用量超过容量阈值时采取跟进措施，比如启动资源补给程序。

16. 供应商管理

阿里云制定了《阿里云供应商信息安全管理规定》和《外包管理制度》，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，进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。

根据《阿里云供应商管理政策》中规定的背景调查要求和程序，阿里云在适用情况下对供应商进行背景调查。阿里云已在合同中指明了权利和义务、服务范围、保密条款、合规要求以及服务等级。供应商必须在开始工作前签署合同。此外，供应商在完成关于信息安全意识的培训后必须通过数据安全测试。

为阿里云提供服务的供应商主要是数据中心服务提供商，包括提供骨干网的电信服务运营商和提供数据中心设施管理的运营商。阿里云和各数据中心服务提供商签署了服务协议，以确定其责任和义务。此外，该协议所附《服务质量保证书》明确了阿里云对数据中心服务可用性等级、业务关系和服务范围的要求以及信息安全要求。阿里云持续监控数据中心服务提供商的服务水平，以确保数据中心安全稳定运行。数据中心服务提供商向阿里云提交服务水平月度报告，该报告涵盖上个月期间提供的服务、重大事件、维保情况和对阿里云的其他反馈。阿里云会在月度会议上审核月度报告，并将异常情况记录到会议纪要中。阿里云每月对数据中心服务商服务水平进行一次评估并发布评估报告，确保服务商符合阿里云的所有要求。

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 ISO 20000 和 ISO 27000 系列标准，至少每年开展一次内部审计。开展内部审计前，内部审计团队制定年度审计计划并获得团队负责人的批准。内部审计团队根据获批的审计计划开展审计工作并编制内部审计报告。外部审计每年由独立第三方进行，审计计划每年根据公司、法律和监管要求的变化而调整。

阿里云致力于持续改进其内部控制体系，以满足新的行业标准。内部审计团队会定期跟进内部和外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。

阿里云在全球运营和维护，遵守国际信息安全标准，也遵守所提供云产品和服务的地区内的信息安全标准。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信任中心。

18. 互操作性和可移植性

阿里云为开发者、企业及合作伙伴提供了一个集服务和组件于一体的开放平台，便于其有效地开展业务。开放平台上可以下载 API 和软件开发工具包，并且可以访问有用的开发文档，支持用户进行运营管理和数据迁移。

阿里云 API 网关支持基于 HTTPS 加密的 API 请求。在管理控制台有不同的 HTTPS 安全策略可供选择。

19. 用户机构补充控制

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，以实现特定的控制目标。仅凭阿里云实施的控制无法有效地实现控制目标。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，以实现只有在合理设计和有效运行补充控制的情况下才能实现的特定控制目标。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。下表不是也不意图包含为用户机构提供控制基础的完整控制列表。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	用户机构的责任
组织安全	• 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、程序和标准以指导其组织内信息安全管理和运行流程。 • 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	• 用户机构应实施适当控制，以确保应用层控制（例如职责分离、自动应用控制、系统计算、报告、系统接口）的设计和运行有效性。
访问管理	• 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。 • 阿里云通过客户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）被准确填写和及时更新，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。 • 用户机构应强化实例的防火墙策略。 • 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，以限制访问存储在阿里云上的数据的权限。 • 用户机构应定期审核对其云资源的访问权限和授权 IP。 • 用户机构应针对敏感活动、系统错误、数据更改等情况，启用和配置适当的记录功能，以支持监控控制和事件响应流程。
数据安全	• 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 轮换机制。 • 用户机构应根据具体要求实施和维护加密选项。
变更管理	• 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，避免生产系统被用于开发活动。

故障管理	• 用户机构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，并支持阿里云进行及时地事件响应。
业务连续性管理	• 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。

第四节—— 阿里云对其控制目标和相关控制的描述，以及独立服务审计师对控制测试和结果的描述

阿里云对其控制目标和相关控制的描述，以及独立服务审计师对控制测试和结果的描述

简介

本报告提供的与范围内云服务相关的云服务体系描述，旨在协助审计师在结合对用户机构控制了解的前提下，计划针对用户机构财务报表或用户机构财务报告内部控制的审计工作，并对可能受阿里云控制影响的用户机构财务报告认定进行控制风险的评估。

本节描述了阿里云指定的控制目标以及为实现相关控制目标所制定的控制。本节也包含了罗兵咸永道会计师事务为测试管理层认为必要的控制的运行有效性，以为相关控制目标的实现提供合理保证，所执行的检查程序，以及控制测试的结果。在后续页面中对控制目标和相关控制的描述是阿里云的职责。对控制测试程序和测试结果的描述是罗兵咸永道的职责。

我们的检查仅限于本节报告中阿里云指定的控制目标和控制，不延伸至用户机构自身运行的控制。在评估整体内部控制时，各用户机构及其独立审计师有责任将此报告中的信息与用户机构财务报告内部控制一同考虑。阿里云的控制无法弥补用户机构内部控制的无效性。

测试程序描述

阿里云的内部控制是多种因素对建立或增强阿里云的控制有效性共同作用的结果。针对阿里云为实现其控制目标而规定的控制，我们在计划相关测试的性质、时间和范围时考虑了阿里云的控制环境、风险评估流程、监控活动以及信息与沟通等因素。

我们采用询问、观察和检查等程序测试控制活动。我们的测试程序包括询问适当的人员并与管理层确认，观察控制的应用、执行或存在，并检查阿里云能够表明控制执行情况的文件和记录。

评估服务机构提供的信息的可靠性

在使用阿里云提供的信息时，我们通过获取关于信息准确性和完整性的证据，评估其是否足够准确和详细，来衡量该信息是否足够可靠以实现我们评估的目的。我们对控制测试中阿里云提供的信息，（包括其系统生成的报告、搜寻结果和清单）执行了观察和检查程序来评估所使用信息的可靠性。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
AAC_01	阿里云制定了《阿里云信息技术管理体系运行与改进管理规定》，以规范内部审计和流程改进的程序和要求。	1. 询问了相应人员，以了解阿里云内部审计的程序和要求，以及每年审查内部审计政策和程序的流程。 2. 检查了《阿里云信息技术管理体系运行与改进管理规定》，以证实制定了相关的政策和程序以确保根据一致的标准来管理审计工作。 3. 检查了每年审查相关政策的支持性证据，以证实至少每年审查一次《阿里云信息技术管理体系运行与改进管理规定》。	未发现异常情况。
AAC_02	每年制定一次外部审计计划，在执行审计工作之前商定审计时间、审计方法以及计划的审计活动，并经授权人员批准。	1. 询问了相应人员，以了解外部审计计划的审批流程以及执行和沟通。 2. 检查了阿里云的年度外部审计计划，以确认内部审计团队在年度审计工作启动之前即已制定了外部审计计划并获得了授权人员的批准。	未发现异常情况。
AAC_03	每年至少根据核准的审计计划开展一次内部审计。审计团队报告审计发现，由管理层进行审核。及时采取跟进措施以修复问题。	1. 询问了相应人员，以了解内部审计计划的审批流程以及执行和沟通情况。 2. 检查了阿里云的年度审计计划，以确认内部审计团队在年度审计工作启动之前即已制定了审计计划并通过了内部审计团队负责人的批准。 3. 检查了内部审计报告和修复记录，以确认阿里云对其内部控制系统的运行开展了内部审计，编制了内部审计报告，且管理层审核并评估了阿里云的内部审计结果并跟踪修复状态。	未发现异常情况。
AIM_01	阿里云制定了《阿里云信息资产安全管理规定》，以规范信息资产的识别、分类和管理。	1. 询问了相应人员，以了解阿里云既定用以规范资产管理程序的信息资产安全管理规定，以及每年审查资产管理政策和程序的流程。 2. 检查了《阿里云信息资产安全管理规定》及相关支持文	未发现异常情况。

控制目标 **1:** 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		档，以确认制定了正式的政策和程序来管理信息资产的管理程序，包括标识、分类、清单开列、可接受的使用、处置等，以确保通过定期的自动更新流程来保证库存始终完整、准确、及时和一致。信息资产需加 以识别、盘点，并分类为人员、硬件、软件、数据和服务。每年审查一次信息资产的识别和分类。 3. 检查了每年审查相关政策的支持性证据，以证实至少每年审查一次资产管理政策。	
AIM_03	新设备的采购必须获得财务部门和产品团队的授权。在部署设备前，必须获得采购批准，通过资产测试，并记录测试结果。	1. 询问了相应人员，以了解设备采购和部署流程。 2. 检查了已部署设备样本的设备采购批准和测试记录，以确认部署设备在部署之前已获得采购批准，并经过测试。	未发现异常情况。
AIM_04	阿里云制定了《采购指引》，以规范设备采购和部署程序的要求。	1. 询问了相应人员，以了解阿里云既定用以规范设备采购和部署程序的采购指引，以及每年审查设备管理政策和程序的流程。 2. 检查了《采购指引》及相关支持文档，以确认制定了正式的政策和程序，以确保根据一致的标准来管理设备采购和部署程序。 3. 检查了每年审查相关政策的支持性证据，以证实至少每年审查一次设备管理政策。	未发现异常情况。
APD_02	阿里云制定了《阿里云操作安全管理规定》，以规范访问权限请求者、访问权限批准者与访问权限管理系统管理员之间的职责分离。	1. 询问了相应人员，以了解阿里云根据既定的操作安全管理政策规范访问权限管理流程中的职责分离的情况，以及每年审查相关政策和程序的流程。 2. 检查了相关政策文档，以确认制定了正式的政策和程序以确保访问权限请求者、访问权限批准者与访问权限管理系统管理员之间的职责分离。	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次相关政策，且必要时根据审查结果更新政策。	
EKM_02	阿里巴巴集团制定了《阿里巴巴集团数据安全规范》，明确了敏感数据的定义和对保护措施的要求，包括对敏感数据使用加密协议。	1. 询问了相应人员，以了解阿里云使用加密协议保护敏感数据的政策，以及每年审查相关政策的流程。 2. 检查了数据安全规范，以确认制定了相关政策和程序明确定义敏感数据以及确保遵照一致的标准使用加密协议来保护敏感数据。 3. 检查了每年审查相关政策的支持性证据，以证实至少每年审查一次与数据安全与加密相关的政策并在必要时更新。	未发现异常情况。
EKM_03	客户可在管理控制台管理其访问密钥。访问密钥在控制台被调用时，会向客户提供有关访问密钥使用的安全提示和最佳操作。	1. 询问了相应人员，以了解客户在管理控制台管理访问密钥的流程。 2. 检查了访问密钥管理流程，以确认客户可以登录到 RAM 控制台创建、禁用或删除其访问密钥。 3. 检查了密钥管理流程，以确认在控制台调用访问密钥时，有关访问密钥使用的安全提示和最佳操作会在屏幕上弹出。	未发现异常情况。
ELC_01	阿里巴巴集团制定了《商业行为守则》，以反映集团愿景和价值观。该守则确立了高级管理层的基调，阐明了道德价值观的重要性以及各级员工维护阿里巴巴集团价值观的总体责任。	1. 询问了相应人员，以了解阿里巴巴集团《商业行为守则》中反映的阿里巴巴集团价值观，以及如何确保员工在该守则发生变更后及时确认知悉变更。 2. 检查了《商业行为守则》，以确认阿里巴巴集团制定了《商业行为守则》用以阐明道德价值观的重要性以及各级员工维护阿里巴巴集团价值观的总体责任。	未发现异常情况。
ELC_02	阿里巴巴集团《商业行为守则》定义了员工的社会责任、对集团的责任、保密义务、法律和法规合规	1. 询问了相应人员，以了解阿里巴巴集团《商业行为守则》对员工提出的要求，以及如何确保员工在该守则发	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	性、道德行为和支持内部控制体系运行的行为。管理层根据需要对《商业行为守则》进行审查和更新。	生变更后及时确认知悉变更。 2. 检查了《商业行为守则》，以确认阿里巴巴集团制定了《商业行为守则》用以定义员工的道德行为、对集团的责任、保密义务、法律和法规合规情况，以及违反安全政策的惩戒措施。 3. 检查了审查和（或）更新记录，以确定管理层在必要时会审查和更新《商业行为守则》。	
ELC_03	员工必须了解《商业行为守则》，并每年完成一次《商业行为守则》在线测试。	1. 询问了相应人员，以了解阿里巴巴集团《商业行为守则》，以及每年完成一次《商业行为守则》在线测试的要求。 2. 检查了阿里巴巴集团《商业行为守则》考试记录的样本，以确认阿里巴巴集团要求员工了解《商业行为守则》并完成《商业行为守则》在线测试。	未发现异常情况。
ELC_04	阿里云每 6 个月开展一次内部员工绩效评估，包括根据《商业行为守则》中定义的标准评估员工道德和价值观。	1. 询问了相应人员，以了解内部员工绩效评估的管理程序。 2. 检查了内部员工绩效管理记录的样本，以确定阿里巴巴集团开展了内部员工绩效评估。	未发现异常情况。
ELC_05	阿里巴巴集团制定了《阿里巴巴集团员工纪律规定》，旨在针对违反安全政策的情况制定相应惩戒措施，并给出了违规行为的分类标准和相应的处罚规定。	1. 询问了相应人员，以了解违反安全政策时的惩戒措施，以及每年审查纪律政策和程序的流程。 2. 检查了《阿里巴巴集团员工纪律规定》，以确认阿里巴巴集团制定了正式政策用以确保指示和法律规定的公开透明，并规范违反安全政策情况下的纪惩戒措施、违规行为的分类标准和相应的处罚规定。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次《阿里巴巴集团员工纪律规定》。	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
ELC_06	阿里云组建了独立的阿里云数据安全团队，以监控和识别员工违规行为。建立了可支持匿名或保密通信的内外部通信渠道。	1. 询问了相应人员，以了解用于独立监控和识别员工违规行为的现行检查机制以及员工违规时的沟通程序。 2. 检查了反腐败平台上举报渠道的屏幕截图以及阿里云数据安全小组的联系信息，以确保制定了相关机制用于监控和识别安全政策之下的员工违规，并建立了沟通渠道用于内部用户和客户进行匿名或机密通信。	未发现异常情况。
ELC_07	违反《商业行为守则》和安全政策的员工将接受调查，已确认的违规情况和处罚决定将汇总在阿里云数据安全违规通知的季度报告中，并由阿里云数据安全团队通过电子邮件面向阿里云全体内部人员发布。	1. 询问了相应人员，以了解调查和处罚员工违反《商业行为守则》和安全政策行为的流程。 2. 检查了通知报告样本，包括阿里云数据安全团队通过电子邮件发布的违规行为和处罚决定，以确认遵照一致的标准对员工违反《商业行为守则》和安全政策的行为进行检查和处罚。	未发现异常情况。
ELC_08	董事会包括独立董事、非独立董事和主席。董事会设立了三个委员会，即审计委员会、薪酬委员会和提名及公司治理委员会。各委员会由专业的董事组成。提名及公司治理委员由主席和 2 名独立董事组成，定期评估各董事的能力和经验。	1. 询问了相应人员，以了解董事会架构和定期评估董事能力的流程。 2. 检查了阿里巴巴网站上的官方披露文件，以确认董事会包括独立董事、非独立董事和主席；董事会设立了三个委员会，即审计委员会、薪酬委员会和提名及公司治理委员会；提名及公司治理委员会定期评估各董事的能力和经验。	未发现异常情况。
ELC_09	董事会每季度召开一次董事会会议。高级管理层在会议上报告与战略事项相关的重大问题和治理情况。董事会通过讨论提供并补充其专业意见。	1. 询问了相应人员，以了解季度董事会会议的组织和内容。 2. 检查了董事会会议记录的样本，以确认董事会定期举行董事会会议。高级管理层在会议期间报告重大问题。	未发现异常情况。
ELC_10	公司建立了针对所有人员层级（包括所在部门和地区信息）的组织架构和清晰的汇报关系，相关信息在阿里巴巴内联网向全体员工开放。	1. 询问了相应人员，以了解人员层级（包括所在部门和地区信息）的组织架构是如何建立的。 2. 检查了组织架构和汇报关系，以确认建立了针对所有人	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		员层级（包括所在部门和地区信息）的组织架构并明确汇报关系。相关架构信息在阿里巴巴内联网上向全体员工开放。	
ELC_11	新员工入职和供应商签约之前，根据《阿里云人力资源安全管理规定》和《供应商管理政策》规定的要求和程序进行背景调查。	1. 询问了相应人员，以了解针对将入职员工的背景调查政策和程序，以及针对供应商的身份验证管理程序。 2. 检查了《阿里云人力资源安全管理规定》和《供应商管理政策》，以确认阿里云制定了正式政策，以规范新员工的背景调查程序和供应商员工的身份验证程序。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次《阿里云人力资源安全管理规定》和《供应商管理政策》。 4. 检查了人力资源管理系统和外包管理系统的背景调查记录样本，以确定阿里云对内部和外部员工的背景进行了相应的调查。	未发现异常情况。
ELC_12	阿里云建立了以下培训体系： • 在相应地区提供内部产品和行业培训，帮助员工掌握工作相关知识； • 向内部技术人员提供云相关的专业考试和培训，以保持技术能力； • 内部员工完成信息安全意识的入职培训后，必须通过商业行为守则和数据安全年度测试； • 供应商员工完成信息安全意识的入职培训后，必须通过数据安全测试； • 安全部门根据需要向员工传达安全意识。	1. 询问了相应人员，以了解针对内部及供应商员工的信息安全意识培训的要求和程序，以及安全部门通告相关要求和程序的方式。 2. 检查了《商业行为守则》和数据安全测试记录的样本，以确认新入职内部员工完成了信息安全意识的入职培训并通过了《商业行为守则》和数据安全的年度考核，供应商员工完成了信息安全意识的培训并通过了数据安全考核，且现有员工每年都会完成《商业行为守则》和数据安全考核。 3. 检查了安全部门与员工之间通信的样本，以确认安全部门会根据需要传达安全意识。	未发现异常情况。
ELC_13	员工（包括内部和供应商员工）的职位、所属部门、主管以及工作职责的相关信息均在内部平台上	1. 询问了相应人员，以了解各部门安全接口人的工作职责以及员工工作职责、所属部门和主管信息的维护情况。	未发现异常情况。

控制目标 1: 公司层面控制

控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证

控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	进行维护	2. 检查了内部平台上的员工信息，以确认阿里云利用该平台来记录和维护有关员工工作职责和汇报关系的信息。	
ELC_14	阿里云制定了《阿里云信息安全风险评估管理规定》，以规范信息安全风险管理流程。	1. 询问了相应人员，以了解信息安全风险评估的政策要求以及每年审查信息安全风险评估政策和程序的流程。 2. 检查了《阿里云信息安全风险评估管理规定》，以确认阿里云制定了正式的政策用于规范信息安全风险管理流程。 3. 检查了每年审查相关政策的支持性证据，以证实至少每年审查一次《阿里云信息安全风险评估管理规定》。	未发现异常情况。
ELC_15	阿里云制定了《阿里云信息安全风险评估管理规定》，以规范信息安全风险识别与评估程序、风险分类的方式、风险承受能力的定义、风险超出承受范围时的解决程序以及风险评估的频率和范围。	1. 询问了相应人员，以了解信息安全风险评估的政策要求以及每年审查信息安全风险评估政策和程序的流程。 2. 检查了《阿里云信息安全风险评估管理规定》，以确认该政策中涵盖了信息安全风险识别与评估程序、风险分类的方式、风险承受能力的定义、风险超出承受范围时的解决程序以及风险评估的频率和范围。 3. 检查了每年审查相关政策的支持性证据，以证实至少每年审查一次《阿里云信息安全风险评估管理规定》。	未发现异常情况。
ELC_16	阿里云至少每年开展一次全面的风险评估，评估时考虑一系列信息安全相关的因素，并根据评估结果更新安全控制措施及相关政策。	1. 询问了相应人员，以了解开展信息安全评估并根据评估结果更新安全控制措施及相关策略的程序。 2. 检查了阿里云信息安全风险评估报告和管理会议纪要，以确认阿里云每年开展信息安全风险评估并根据评估结果更新和完善安全政策和控制措施。 3. 检查了合规团队的解决计划，其中包含有关跟进行动、负责人和计划完成日期的详细信息，以确认合规团队已被告知已识别风险的状态和缓解性保护措施。	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
ELC_17	信息管理指导委员会每月组织业务部门及风险与合规部门的领导讨论业务更新、政策更新、技术环境变化及其影响。	1. 询问了相应人员，以了解信息管理指导委员会月度会议的情况。 2. 检查了信息管理指导委员会月度会议记录的样本，以确认各业务部门及风险与合规部门的领导探讨了业务更新、政策更新、技术环境变化及其影响。	未发现异常情况。
ELC_18	阿里云制定了《阿里云信息技术管理体系政策和目标》，以规范信息安全及个人信息管理的总体策略和目标。	1. 询问了相应人员，以了解信息安全及个人信息管理的总体策略和目标，以及每年审查相关政策和程序的流程。 2. 检查了《阿里云信息技术管理体系政策和目标》，以确认阿里云制定了正式政策，用于规范信息安全及个人信息管理总体策略和目标。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次《阿里云信息技术管理体系政策和目标》。	未发现异常情况。
ELC_19	阿里云制定了《阿里云信息技术管理体系组织架构》，旨在定义信息技术管理体系内部成员和事业部（包括领导团队、内部审计团队和工作组）的职责。	1. 询问了相应人员，以了解信息安全管理体系、信息安全管理体系内部成员和事业部的职责，以及每年审查相关政策和程序的流程。 2. 检查了《阿里云信息技术管理体系组织架构》，以确认阿里云制定了正式政策用以明确信息安全组织架构内部成员和事业部（包括领导团队、内部审计团队和工作组）的职责。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次《阿里云信息技术管理体系组织架构》。	未发现异常情况。
ELC_20	员工可在阿里云内部平台上查询相关政策。	1. 询问了相应人员，以了解员工查询信息安全政策的内部平台，包括阿里巴巴的信息安全管理体系 （ISMS） 与 IT 服务管理体系 （ITSM） 政策架构，以及审查、更新、审批政策的流程和涉及的相关方。 2. 检查了阿里云的内部平台，以确认政策已传达给所有内	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		部员工且对其开放。 3. 检查了阿里云的 ISMS 与 ITSM 政策，以确认政策经过核心部门按统一的结构进行审查、更新。	
ELC_21	阿里云制定了《阿里云信息技术管理体系组织架构》，旨在定义各部门安全接口人工作职责，并实施政策中定义的信息安全机制，包括建立部门工作标准、监控日常工作中的安全事件以及协调资源以支持信息安全内部审计或风险评估。	1. 询问了相应人员，以了解既定的《阿里云信息技术管理体系组织架构》中所定义的各部门安全接口人工作职责，以及每年审查相关政策和程序的流程。 2. 检查了《阿里云信息技术管理体系组织架构》及相关支持性文件，以确定制定了正式的政策和程序用以明确各部门安全接口人工作职责，包括建立部门工作标准、监控日常工作中的安全事件以及协调资源以支持信息安全内部审计或风险评估。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次信息技术管理政策。	未发现异常情况。
ELC_22	阿里云制定了《阿里云人力资源安全管理规定》，以规范新员工和第三方人员参与信息安全意识培训的要求。	1. 询问了相应人员，以了解既定的《阿里云人力资源安全管理规定》中对新员工和第三方人员开展信息安全意识培训提出的要求，以及每年审查相关政策和程序的流程。 2. 检查了《阿里云人力资源安全管理规定》及相关支持文档，以确认制定了正式的政策和程序以规范新员工和第三方人员参与信息安全意识培训的要求。 3. 检查了每年审查相关政策的支持性证据，以证实至少每年审查一次《阿里云人力资源安全管理规定》。	未发现异常情况。
ELC_23	阿里云制定了《阿里云信息安全法律法规符合性管理规定》，旨在规范监管政策更新收集以及与外部各方联的络机制。阿里云的官方网站上有在线新闻中心和公告栏，用于发布最新商业新闻、安全警报、服务变更、监管更新等。	1. 询问了相应人员，以了解既定的《阿里云信息安全法律法规符合性管理规定》中所规定的监管政策更新收集以及与外部各方联络的机制，以及每年审查相关政策和程序的流程。	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		2. 检查了《阿里云信息安全法律法规符合性管理规定》和相关支持性文件，以确认制定了正式的政策和程序用以规范获得监管政策更新的机制。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次信息安全法律法规符合性管理政策。 4. 检查了阿里云官网上的在线新闻中心和公告栏，以确认阿里云利用该新闻中心和公告栏向股东、合作伙伴、监管机构、客户、财务分析师和其他外部各方提供相关信息更新。	
ELC_24	阿里云制定了《阿里云人力资源安全管理规定》，旨在规范员工保密协议签署程序以及明确员工遵守信息安全相关政策的责任。	1. 询问了相应人员，以了解既定的《阿里云人力资源安全管理规定》中所定义的员工信息安全责任和规范保密协议签署程序，以及每年审查相关政策和程序的流程。 2. 检查了《阿里云人力资源安全管理规定》及相关支持性文件，以确认制定了正式的政策和程序用以规范员工保密协议签署流程以及明确员工遵守信息安全相关政策的责任。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次人力资源安全管理规定。	未发现异常情况。
ELC_25	阿里云制定了《阿里云人力资源安全管理规定》，规范法务部门在维护员工、第三方以及业务合作伙伴的保密协议模板方面的责任。阿里云法务部门至少每年审核和更新一次保密协议中的法律规定。	1. 询问了相应人员，以了解是否按照《阿里云人力资源安全管理规定》管理用于流程维护的保密协议模板，以及每年审核相关政策和程序的流程。 2. 检查了《阿里云人力资源安全管理规定》和其他支持文档，以确定制定了正式的政策和程序以规范法务部门在更新和维护员工和第三方保密协议模板方面的责任。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年对人力资源安全管理政策进行审查。	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		4. 检查了每年审查保密协议模板的支持性证据，以验证法务部门至少每年对保密协议模板进行审查。	
ELC_26	阿里云在劳动合同、保密协议和声明书中明确了内部员工在信息安全方面的责任和义务。内部新员工需要签署劳动合同、保密协议和声明书。供应商员工需要提供与所属供应商签署的保密协议。	1. 询问了相应人员，以了解针对内部新员工签署劳动合同、保密协议和声明书,以及针对新供应商员工签署保密协议制定的相关规定。 2. 检查了所签署的劳动合同、保密协议和声明书的样本，以确认内部新员工已签署用于确定员工在信息安全方面的责任和义务的劳动合同、保密协议和声明书。 3. 检查了所签署的保密协议的样本，以确认新供应商员工已与所属供应商签署用于确定员工保密义务的保密协议。	未发现异常情况。
ELC_27	阿里云通过管理控制台、电子邮件和短信建立了与客户沟通的渠道，用于向客户通知可能对其有影响的所有事件。	1. 询问了相应人员，以了解阿里云制定的与客户的通信协议。 2. 检查了管理控制台中发布的通知信息，以及发送给客户的涉及安全事件的电子邮件和短信，以确认阿里云制定了通过管理控制台、电子邮件和短信与客户沟通的通信协议，用于向客户通知所有可能对其有影响的任何事件。	未发现异常情况。
ELC_28	阿里云在管理控制台中提供了工单服务，供客户向阿里云报告与安全性、可用性和保密性相关的故障、事件、疑虑和投诉。	1. 询问了相应人员，以了解通过管理控制台工单系统提供客户支援的流程，以及事件处理流程中的客户参与情况。 2. 检查了管理控制台中的工单服务，以确认客户能够向阿里云报告问题。 3. 检查了事件处理系统，以确认该系统能够支持对事件的评估，能够向云客户通知或告知相关事件，以及能够为负责处理事件的部门提供支持并保留处理记录。其中还包括根据合同协议的规定以常规的适当形式向客户告知	未发现异常情况。

控制目标 **1:** 公司层面控制

控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证

控制 ID	阿里云的控制描述	PwC 的测试程序	PwC 的测试结果
		对其有影响的事件的状态，并在事件得到纠正后立即向客户告知所采取保护措施。	
ELC_29	阿里云在服务协议中规定了客户和阿里云各自的责任和义务，其中包括阿里云提供的服务类型和等级，保密协议和数据披露条款，以及监管部门的检查权。客户在使用相关产品服务之前需确认并同意相关服务协议或产品条款。	1. 询问了相应人员，以了解阿里云产品服务的获取流程，以及制定的相关服务协议和产品条款。 2. 检查了阿里云产品服务获取流程以及服务协议和产品条款，以确认服务协议和产品条款恰当界定了客户和阿里云各自的责任和义务，包括阿里云提供的服务类型和等级，保密条款和数据披露条款，以及监管部门的检查权，且客户需在获取相关阿里云产品服务之前确认并接受相关协议和条款。	未发现异常情况。
ELC_30	财务预算由财务部及财务规划与分析团队制定。随后由首席执行官和首席财务官根据阿里巴巴集团的运营目标审查并调整财务预算及关键绩效指标（KPI）。	1. 询问了相应人员，以了解阿里巴巴集团为各事业部和公司部门设定适当的财务预算和 KPI 的程序。 2. 检查了各事业部的最终财务预算和 KPI 以及审批记录，以确认财务部及阿里巴巴集团的财务规划与分析团队编制了预算和 KPI，并由首席执行官和首席财务官根据阿里巴巴集团的运营目标进行适当地审查和调整。	未发现异常情况。
ELC_31	阿里巴巴集团根据适用的会计准则建立了内部控制框架以确保实现财务报告目标。针对各项关键业务流程，通过考虑流程的重要性及其他定性和定量因素以识别并评估与财务报告目标相关的风险。采用专门设计的内部控制来应对所识别的风险。	1. 询问了相应人员，以了解用于风险识别和评估的内部控制，以及设计相应的内部控制以应对所识别的风险。 2. 检查了风险控制矩阵，以确认与各项关键业务流程的财务报告目标相关的风险在阿里巴巴集团的内部控制框架下被识别并处理。	未发现异常情况。
ELC_32	阿里巴巴集团根据适用的会计准则确定了会计程序和财务报告的控制目标。控制的设计和实施可确保会计信息反映公司的业务活动和运营情况，并确保所有关键事项均被识别并在外部报告中披露。	1. 询问了相应人员，以了解通过既定的财务报告和信息披露程序确保遵守适用会计准则的情况。 2. 检查了财务报告（包括管理层的估计、年度报告和披露项目）的风险控制矩阵，以确认阿里巴巴集团建立了有效的控制措施，以确保会计信息准确反映公司的业务活动和运营情况，并确保所有关键事项均被识别并在外部	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		报告中披露。	
ELC_33	阿里巴巴集团联合其他公司共同成立了反欺诈联盟，以通过共享信息来应对欺诈活动。	1. 询问了相应人员，以了解用于应对欺诈活动的反欺诈控制措施和机制的建立情况。 2. 检查了中国反欺诈联盟的网页，以确认阿里巴巴集团已建立反欺诈机制来应对欺诈活动，并且与外部各方共享与欺诈活动相关的信息以防止欺诈活动。	未发现异常情况。.
ELC_34	阿里巴巴集团组建了专门的法律团队，负责审查与各个事业部相关的国内外法律法规，识别相关的合规风险并解决法律纠纷。建立了共享法律服务中心，以宣传与遵守法律法规相关的知识，并为集团达到合规目标提供支持。	1. 询问了相应人员，以了解用于识别合规风险和法律纠纷的合规管理程序。 2. 检查了集团有限公司的法律平台以及相关部门提供的涉及法律法规纠纷的证据，以确认阿里巴巴集团组建了专门的法律团队并建立了共享法律服务中心，以宣传与遵守法律法规相关的知识，并为集团提供相关的支持。	未发现异常情况。
ELC_35	阿里巴巴集团提倡一种积极应对外部环境变化和市场变化的战略。	1. 询问了适当人员，以了解阿里巴巴集团应对外部环境和市场变化的公司战略。 2. 检查了首席执行官提出的公司战略，以确认阿里云识别并分析了可能对财务报告、开发、运营和安全产生重大影响的业务变化。	未发现异常情况。
ELC_36	阿里巴巴集团的业务模式和运营模式根据外部环境和公司的发展情况加以调整。	1. 询问了相应人员，以了解阿里巴巴集团根据外部环境和的公司战略调整业务模式和运营模式的情况。 2. 检查了业务和运营模式的调整情况，以确认阿里巴巴集团会确定外部环境的变化并根据公司战略调整其业务和运营模式。	未发现异常情况。
ELC_37	阿里巴巴集团设立了专门的举报电子邮箱，用于接收员工诚信问题的报告。	1. 询问了相应人员，以了解接收员工诚信问题报告的举报机制。	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		2. 检查了诚信合规网页，以确认阿里云建立了用于接收员工诚信问题报告的举报机制。	
ELC_IoT_38	<u>适用于物联网平台</u> 客户通过阿里云物联网平台下载其物联网设备的 productKey、deviceName 和 deviceSecret 信息时，下载页将向客户发出风险预警。风险预警中规定了客户在将 productKey、deviceName 和 deviceSecret 信息下载到本地后对妥善保护此等信息的责任，并提供了相关的安全建议。	1. 询问了相应人员，以了解客户开始在阿里云物联网平台的网页上下载设备信息（productKey、deviceName、deviceSecret）时向客户提供风险预警的机制。 2. 检查了阿里云物联网平台的设备信息（productKey、deviceName、deviceSecret）下载页面，以确认在设备信息下载页面中启用了风险预警机制。且风险预警中明确规定了信息保护责任和相关的安全建议。	
STA_01	阿里云制定了《阿里云供应商信息安全管理规定》和《供应商管理政策》，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。	1. 询问了相应人员，以了解既定的《阿里云供应商信息安全管理规定》和《供应商管理政策》中所规定的供应商和第三方员工全流程管理要求，以及每年审查相关政策和程序的流程。 2. 检查了《阿里云供应商信息安全管理规定》和《供应商管理政策》及相关支持性文件，以确认制定了正式的政策和程序，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。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次供应商管理政策。	未发现异常情况。
STA_02	要求供应商签订合同，且合同内容涵盖双方的权利和义务、服务范围、保密条款、合规性要求和服务水平。	1. 询问了相应人员，以了解确保新供应商签订了合同的流程。 2. 检查了为云服务提供相关服务的供应商样本的合同，以确认供应商签订了合同，且合同内容涵盖双方的权利和义务、服务范围、保密条款、合规性要求和服务水平。	未发现异常情况。
STA_03	阿里云每月根据合同中规定的合规性要求和服务水平评估供应商绩效。	1. 询问了相应人员，以了解阿里云根据既定的供应商绩效评估程序规范供应商绩效管理的情况。 检查了数据中心样本的服务水平评估报告，以确认开展	未发现异常情况。

控制目标 1: 公司层面控制			
控制就组织政策和信息安全政策的制定、传达、实施和监控提供合理保证			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		了每月服务水平评估，包括审核与服务相关的服务报告（如 SLA 报告）、安全相关的事件以及操作中断或故障。对识别出的偏差进行风险分析，并由适当的人员及时跟进。	
STA_04	数据中心服务供应商向阿里云提交月度服务水平报告，其中涵盖前一月提供的所有服务以及对阿里云的所有反馈。阿里云的数据中心经理在月度会议上审核这些月度报告，并将异常情况记录到会议纪要中。	1. 询问了相应人员，以了解阿里云针对监控数据中心服务供应商所提供的服务制定的监控程序。 2. 检查了数据中心样本的服务水平报告和会议记录，以确认阿里云在月度会议上收集并审查了数据中心服务供应商编制的月度服务水平报告，并将异常情况记录到会议纪要中。	未发现异常情况。

控制目标 2: 基础架构和虚拟化安全			
控制合理保证了云服务的基础设施配置和虚拟化技术的使用安全。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
AIM_02	阿里云建立了配置管理数据库，用于维护与云服务相关的信息资产。盘存的各项信息资产均分配了资产归属人。信息资产的更改也会记录在数据库中。	1. 询问了相应人员，以了解配置管理数据库如何管理与云服务相关的信息资产。 2. 检查了信息资产样本的在配置管理数据库中的清单信息，以确认对资产进行了盘存，记录了资产更改历史，且所有盘存资产均分配了云服务提供商方面的负责人。	未发现异常情况。
IVS_01	阿里云制定了《阿里云网络安全管理政策》，要求生产环境与非生产环境相隔离并归入不同的网络安全域。	1. 询问了相应人员，以了解既定的《阿里云网络安全管理政策》中提出的生产环境与非生产环境的隔离要求。 2. 检查了《阿里云网络安全管理政策》，以确认通过不同的网络安全域将生产环境与非生产环境相隔离。	未发现异常情况。
IVS_02	阿里云建立了网络拓扑图，以展示相关的网络架构和数据流。	1. 询问了相应人员，以了解网络拓扑图中相关的网络架构和数据流。	未发现异常情况。

控制目标 2: 基础架构和虚拟化安全 控制合理保证了云服务的基础设施配置和虚拟化技术的使用安全。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		2. 检查了网络拓扑图，以确认该图体现了生产网络、办公网络和数据流。	
IVS_03	通过防火墙规则，阿里云内联网无法链接互联网。	1. 询问了相应人员，以了解通过配置防火墙实现对公网与内联网进行隔离的情况。 2. 检查了防火墙规则，以确认建立了公网与内联网的隔离。	未发现异常情况。
IVS_04	办公网络和生产网络是相互隔离的。在生产环境中，客户网络和运维网络是相互隔离的。	1. 询问了相应人员，以了解阿里云中网络隔离的情况。 2. 检查了网络访问控制列表，以确认建立了办公网络和生产网络隔离，客户网络与运维网络的隔离。	未发现异常情况。
IVS_05	阿里云通过 IP 白名单对每个相互隔离的网络环境进行访问权限控制。	1. 询问了相应人员，以了解阿里云针对网络隔离实施的跨域访问控制。 2. 检查了网络安全域的 IP 白名单配置，以确认通过 IP 白名单的执行来实现网络隔离。	未发现异常情况。
IVS_06	阿里云实施网络流量分离机制，以确保 ECS 实例无法捕获其他实例的网络流量。阿里云设置了安全组，以实现对 ECS 实例的访问控制。不同安全组中的 ECS 实例默认无法相互访问，但可以通过配置安全组规则来控制对 ECS 实例的网络访问权限。	1. 询问了相应人员，以了解 ECS 实例的网络流量分离和安全组访问控制的机制。 2. 检查了安全组机制，以确认不同安全组中的 ECS 实例默认无法相互访问，且可配置安全组规则控制 ECS 实例的网络访问权限。	未发现异常情况。
IVS_07	阿里云在网络边界部署了云安全及其系统组件，以检测和防御 DDoS 攻击。	1. 询问了相应人员，以了解阿里云对 DDoS 攻击的检测和防御机制。 检查了部署在网络边界的检测平台和防御机制，以确认实施了适当的保护以防御 DDoS 攻击。	未发现异常情况。

控制目标 2: 基础架构和虚拟化安全			
控制合理保证了云服务的基础设施配置和虚拟化技术的使用安全。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
IVS_08	阿里云使用网络监控平台根据预定义的规则实时监控网络流量和用户操作。根据监控结果生成自动警报并发送给安全团队进行调查。	1. 询问了相应人员，以了解针对异常网络流量和恶意用户操作设置的监控程序。 2. 检查了监控平台发送的警报样本，以确认恰当审查并解决了异常网络流量或恶意用户操作。	未发现异常情况。
IVS_09	在部署虚拟机镜像变更之前应在变更管理平台提出请求并得到批准。验证方法和结果也应当记录在变更平台中。阿里云通过官网与客户沟通已发布的变更。	1. 询问了相应人员，以了解虚拟机镜像的变更管理流程。 2. 检查了虚拟机镜像的变更样本，以确认变更在实施之前经过适当测试和批准，验证结果已记录，并通知客户变更情况。	未发现异常情况。
IVS_ECS_10	**适用于 ECS** ECS 实例通过绑定 IP 地址，防止 IP 地址欺骗。	1. 询问了相应人员，以了解将固定的内网 IP 地址分配给各 ECS 实例的机制。 2. 检查了 ECS 实例与另一个 ECS 实例和公网的连接，以确认通过预先分配的 ECS IP 地址连接成功。 3. 检查了使用修改后的 IP 地址连接 ECS 实例至另一个 ECS 实例和公网，以确认使用修改后的 ECS IP 地址连接失败，并且确认已对内联网 IP 地址修改进行限制，以确保免受 IP 欺骗攻击。	未发现异常情况。
IVS_IoT_11	**适用于物联网平台** 客户创建产品后，物联网平台会为不同产品分配带有其唯一 productKey 的域名。由于每个产品的 productKey 是唯一的，在客户通过域名访问产品时，产品之间实现了逻辑隔离以防止访问其他产品数据的情况发生。	1. 询问了相应人员，以了解有关产品层面的逻辑隔离机制，以防止阿里云物联网平台产品间的未授权数据访问。 2. 通过后端系统检查了产品相关的 productKey 生成机制，以确定在 productKey 生成流程中使用了随机序列生成工具。 3. 通过后端系统检查了产品域名生成机制，以确定在域名生成流程中使用了 productKey 信息，从而确保不同产品之间的逻辑隔离。	未发现异常情况。

控制目标 **2:** 基础架构和虚拟化安全			
控制合理保证了云服务的基础设施配置和虚拟化技术的使用安全。			
控制 ID	阿里云的控制描述	**PwC** 的测试程序	**PwC** 的测试结果
IVS_ECS_12	**适用于 ECS** 当通过虚拟机镜像创建 ECS 实例时，阿里云将会进行完整性检查以保护镜像免受恶意篡改。	1. 询问了相应人员，以了解通过虚拟机镜像创建 ECS 实例期间的完整性检查流程，以保护镜像免受恶意篡改。 2. 检查了通过虚拟机镜像创建 ECS 实例时使用的验证码和完整性检查日志，以确认完整性检查流程成功执行。 3. 检查了由于完整性检查失败而导致 ECS 实例创建失败时生成的完整性检查日志，以确认完整性检查失败时会显示错误信息。	未发现异常情况。.
IVS_RDS_13	**适用于 RDS** 客户被禁止通过加载动态链接库在主机操作系统内执行命令。	1. 询问了相应人员，以了解防止通过加载动态链接库在 RDS 主机操作系统内执行命令的机制。 2. 检查了通过加载动态链接库在主机操作系统内执行命令的流程，以确认数据库系统拒绝了动态链接库加载命令，从而防止客户在主机操作系统内执行命令。	未发现异常情况。
IVS_RDS_14	**适用于 RDS** RDS 默认设定为内网连接模式。客户可通过 ECS 实例和管理控制台的 DMS 系统从内网访问 RDS。客户可配置 IP 白名单以防止未经授权的访问 RDS。	1. 询问了相应人员，以了解 RDS 展现的内部连接模式，以确保客户只能通过 ECS 实例和管理控制台的 DMS 系统访问 RDS 实例。客户可根据 IP 地址白名单对 RDS 实例进行访问控制，以拒绝未经授权的访问请求。 2. 检查了通过 DMS 系统登录 RDS 实例的流程，以确认当 DMS 系统的 IP 地址不在白名单中时，登录尝试失败。 3. 检查了通过 DMS 系统登录 RDS 实例的流程，以确认当 DMS 系统的 IP 地址在白名单中时，登录尝试成功。	未发现异常情况。

控制目标 2: 基础架构和虚拟化安全			
控制合理保证了云服务的基础设施配置和虚拟化技术的使用安全。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		4. 检查了通过 ECS 实例登录 RDS 实例的流程，以确认当 ECS 实例的 IP 地址不在白名单中时，登录尝试失败。 5. 检查了通过 ECS 实例登录 RDS 实例的流程，以确认当 ECS 实例的 IP 地址在白名单中时，登录尝试成功。	
IVS_OSS_15	**适用于 OSS** OSS 为客户提供基于存储空间(bucket)和文件的访问控制；当客户新建存储空间后，若不指定权限，OSS 默认为该存储空间设置“私有”权限。只有被授权的其他客户的子账号能够对该存储空间和文件执行操作。	1. 询问了相应人员，以了解在 OSS 产品中创建的存储空间和文件的访问控制。 2. 检查了通过阿里云管理控制台新建存储空间和文件的流程，以确认创建存储空间和文件时必须选择授权类型，且该授权类型默认设置为“私有”。 3. 检查了授予其他客户的特定子账号访问权限的流程，以确认只有被授权的子账号才能够对该存储空间和文件进行操作。	未发现异常情况。
IVS_SLB_16	**适用于 SLB** SLB 提供虚拟 IP 地址以隐藏后端服务器的 IP 地址。	1. 询问了相应人员，以了解阿里云 SLB 提供虚拟 IP 地址以隐藏后端服务器的 IP 地址的情况。 2. 检查了创建一个后端服务器和一个 SLB 实例重新发起访问请求的流程，以确认可以在不知道后端服务器 IP 地址的情况下通过 SLB 公网 IP 成功访问后端服务器。	未发现异常情况。
IVS_VPC_17	**适用于 VPC** 只有与弹性公网 IP 绑定的 ECS 实例可直接访问公网。不同 VPC 之间内部相互隔离，只有通过对外映射的 IP 地址才能相互访问。	1. 询问了相应人员，以了解阿里云 ECS 提供的、用于直接访问公网的弹性公网 IP。位于不同 VPC 内的 ECS 实例相互隔离。位于不同 VPC 内的 ECS 实例只能通过弹性公网 IP 实现互联。 2. 检查了未与弹性公网 IP 绑定的 ECS 实例的创建流程，并试图在 ECS 实例与公网之间建立连接。连接失败。	未发现异常情况。

控制目标 2: 基础架构和虚拟化安全			
控制合理保证了云服务的基础设施配置和虚拟化技术的使用安全。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 检查了 ECS 实例的弹性公网 IP 分配流程，并试图在 ECS 实例与公网之间建立连接。连接成功。 4. 检查了新建 VPC 的流程，并配置了安全组。将 ECS 位置从 VPC1 更改为 VPC2，以使两个 ECS 分别位于两个不同的 VPC 中。配置安全组规则，试图使用私有 IP 将两个安全组相连，但两个连接都失败。 5. 检查了两个弹性公网 IP 的创建流程，并将其分配给相应 ECS。配置安全组规则，试图使用弹性公网 IP 将两个安全组相连，两个连接都成功。	
IVS_NAT_18	**适用于 NAT 网关** NAT 网关提供 SNAT 功能，允许未配置弹性公网 IP 地址或公网地址的内部 ECS 实例连接互联网服务。	1. 询问了相应人员，以了解 NAT 网关的 SNAT 功能。该功能可以为未配置弹性公网 IP 地址或公网 IP 地址的内部 ECS 实例通过 SNAT 功能中提供的公网 IP 地址连接外部服务。 2. 检查了通过管理控制台在 NAT 网关服务中启用 SNAT 功能的流程，然后通过 SNAT 功能中提供的公网 IP 地址从内部 ECS 实例连接，以确认连接成功。 3. 检查了通过使用 SNAT 功能中提供的公网 IP 地址从外部网络连接的流程，以确认连接失败。	未发现异常情况。
IVS_NAT_19	**适用于 NAT 网关** NAT 网关提供 DNAT 功能，通过在 DNAT 内建立公网 IP 地址/端口与 ECS 实例专用 IP 地址/端口之间的映射关系，实现对外部访问请求的访问控制。	1. 询问了相应人员，以了解 NAT 网关的 DNAT 功能。该功能允许外部实体通过建立公网 IP 地址/端口与内部 ECS 实例专用 IP 地址/端口之间的映射关系访问内部 ECS 实例。 2. 检查了未配置弹性公网 IP 地址或公网 IP 地址的 ECS 实例创建流程，对一个简单网页进行了配置，以确认来自外部实体的访问请求不能直接发送至内部 ECS 实例。	未发现异常情况。

控制目标 2: 基础架构和虚拟化安全 控制合理保证了云服务的基础设施配置和虚拟化技术的使用安全。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 检查了 NAT 网关服务中 DNAT 功能的启动流程，然后通过公网 IP 地址对在内部 ECS 实例创建的网页发起外部实体的访问请求，以确认该访问请求成功。	
IVS_EIP_20	**适用于弹性公网 IP** 各弹性公网 IP 与相关租户 ID 之间的关系均在后端数据库系统中维护，以确保一个弹性公网 IP 地址不会同时分配给不同的租户。	1. 询问了相应人员，以了解后端数据库系统中各弹性公网 IP 与相关租户 ID 之间的关系。 2. 检查了后端数据库系统中一个弹性公网 IP 映射至不同的租户 ID 且时间不重叠的参数屏幕截图，以确认一个弹性公网 IP 地址不会同时分配给不同的租户。	未发现异常情况。
IVS_EIP_21	**适用于弹性公网 IP** 建立了异常弹性公网 IP 检测机制，以防止将异常的弹性公网 IP 地址重新分配给其他租户。	1. 询问了相应人员，以了解异常弹性公网 IP 检测机制。 2. 检查了异常 IP 平台中的记录，以确认如果在常规连接检查中检测到异常弹性公网 IP 地址，异常 IP 将被记录在平台上。 3. 检查了后端系统中的记录，以确认如果有弹性公网 IP 地址在常规连接检查中被确定为异常，则该弹性公网 IP 地址将会被标记为已锁定且不会被重新分配给其他租户。	未发现异常情况。
TVM_01	安全团队制定了配置基线标准，其中规定了对操作系统、数据库管理系统、网络设备和虚拟机镜像的基准要求。安全团队每年至少审查并更新一次配置基线标准。	1. 询问了相应人员，以了解针对操作系统、数据库管理系统、网络设备和虚拟机镜像所制定的配置基线标准，以及每年审查并更新配置基线标准的要求。 2. 检查了操作系统、数据库管理系统、网络设备和虚拟机镜像的配置基线标准，以及相关的审查和更新记录，以确认安全团队制定了正式的标准，且每年至少审查一次配置基线标准并相应更新。	未发现异常情况。
TVM_02	阿里云部署了配置扫描工具，用于扫描操作系统、数据库管理系统、网络设备和虚拟机镜像的	1. 询问了相应人员，以了解操作系统、数据库管理系统、网络设备和虚拟机镜像非标准配置的检查和恢	未发现异常情况。

控制目标 **2:** 基础架构和虚拟化安全			
控制合理保证了云服务的基础设施配置和虚拟化技术的使用安全。			
控制 **ID**	阿里云的控制描述	**PwC** 的测试程序	**PwC** 的测试结果
	配置。扫描工具对扫描结果进行分析，并将分析结果自动提交至安全事件和漏洞管理平台。由操作人员检测不满足基线配置标准的情况并将其恢复直至满足标准。检测和恢复结果在每周报告中汇总以进行审查。	复程序。 2. 检查了配置扫描工具中设置的扫描任务及扫描记录，以确认配置扫描工具可自动扫描操作系统、数据库管理系统、网络设备和虚拟机镜像的配置。 3. 检查了内部平台中设置的检测规则，以确认扫描结果由内部平台进行分析，且平台可检测不满足基线文件中规定的标准配置的情况。 4. 检查了每周报告的样本，以确认非标准配置将由操作人员恢复至满足标准，且检查和恢复结果在每周报告中汇总。	
TVM_04	阿里云在物理服务器上安装了入侵检测软件，用于检测潜在的入侵行为。	1. 询问了相应人员，以了解在物理服务器上安装入侵检测软件的规定和相应更新流程。 2. 检查了内部平台中设置以自动扫描入侵检测软件（IDS）并将其推送到物理服务器进行安装（如果物理服务器未配备 IDS ）的脚本任务，以确认这些服务器已安装入侵检测软件以检测潜在的入侵行为。 3. 检查了《阿里云安全运维制度》，以确认入侵防御/检测软件已集成到整个安全信息和事件管理流程中，将这些事件与其他事件相联，启动安全措施。	未发现异常情况。

控制目标 **3:** 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 **ID**	阿里云的控制描述	**PwC** 的测试程序	**PwC** 的测试结果
APD_01	阿里云针对逻辑访问管理制定了《阿里云访问控制管理规定》。该政策要求按照最小授权原则，并且仅在业务需要时授予访问权限。该政策根据公司架	1. 询问了相应人员，以了解阿里云根据最小授权原则和职责分离基本规则建立的访问控制管理规定，以及每年审查相关政策和程序的流程。	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	构定义了按照管理级别和运营级别角色和职能进行职责分离的基本规则。	2. 检查了相关政策文档，以确认制定了正式的政策和程序，以管理系统和数据的访问并规范职责分离。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次相关政策，且必要时根据审查结果更新政策。	
APD_02	阿里云制定了《阿里云操作安全管理规定》，以规范访问权限请求者、访问权限批准者与访问权限管理系统管理员之间的职责分离。	1. 询问了相应人员，以了解阿里云根据既定的操作安全管理政策规范访问权限管理流程中的职责分离的情况，以及每年审查相关政策和程序的流程。 2. 检查了相关政策文档，以确认制定了正式的政策和程序以确保访问权限请求者、访问权限批准者与访问权限管理系统管理员之间的职责分离。 3. 检查了每年审查相关政策的支持性证据，以至少每年审查一次相关政策，且必要时根据审查结果更新政策。	未发现异常情况。
APD_03	阿里云制定了密码策略，包含密码长度、复杂性、历史记录、最小和最大使用期限、账户锁定阈值及更改初始密码的要求。密码根据既定标准在 Active Directory 层面使用，并通过单点登录来实施。	1. 询问了相应人员，以了解阿里云既定的密码配置基线和密码管理程序以确保执行密码要求且安全处理身份验证信息，以及每年审查相关政策和程序的流程。 2. 检查了密码策略的文档，以确认制定了正式的策略，包含密码长度、复杂性、历史记录、最小和最大使用期限、账户锁定阈值及更改初始密码的要求。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次相关政策，且必要时根据审查结果更新政策。	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		4. 检查密码配置设置和密码更改流程，以确认在 Active Directory 层面配置了密码，以根据既定策略执行密码要求。	
APD_04	制定了相关程序，以自动为具有有效 HR 记录的新员工创建 Active Directory 账户。	1. 询问了相应人员，以了解根据人力资源系统信息自动为新员工创建 Active Directory 账户的程序。 2. 检查了创建 Active Directory 账户的系统逻辑，以确认身份验证系统从人力资源系统实时接收员工信息，并自动为具有有效 HR 记录的新员工创建 Active Directory 账户。 3. 检查了身份验证系统为人力资源系统中新入职员工样本创建 Active Directory 账户的创建记录，以确认系统自动在雇佣开始日创建该新入职员工的 Active Directory 账户。	未发现异常情况。
APD_05	阿里云根据员工各自的职位和角色为其提供最小的资源访问权限。所请求的应用生产系统访问权限经授权人员批准后提供。	1. 询问了相应人员，以了解生产环境中应用系统访问权限的申请和审批程序。 2. 检查了生产环境中应用系统访问权限申请和审批样本，以确认应用系统访问权限仅在授权人员批准后根据申请人的职位和角色相应提供，且申请人与批准人之间进行了严格的职责划分。	未发现异常情况。
APD_06	客户在阿里云网站上注册时即会被分配一个唯一的用户账户。	1. 询问了相应人员，以了解在客户注册阿里云账户时即为其分配唯一用户账户的流程。 2. 检查了账户注册流程，以确认管理控制台在客户注册账户时在分配账户之前会自动检查用户账户的唯一性。	未发现异常情况。
APD_07	客户执行自助密码重置时，通过向已验证的手机发	1. 询问了相应人员，以了解客户自助密码重置的程	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	送短信验证码完成客户身份验证。	序。 2. 检查了密码重置程序，以确认客户身份在重置密码前通过向已验证的手机发送短信验证码完成验证。	
APD_08	客户通过 API 访问阿里云资源时，通过访问密钥完成客户身份验证。	1. 询问了相应人员，以了解客户调用云资源 API 时的身份验证过程。 2. 检查了通过调用 API 操作访问阿里云资源的流程，以确认访问云资源时通过访问密钥信息完成身份验证。	未发现异常情况。
APD_09	阿里云为客户提供集中式用户身份管理和资源访问控制服务，供客户控制对其云资源的操作权限。	1. 询问了相应人员，以了解客户控制对其云资源操作权限的流程。 2. 检查了访问管理流程，以确认客户能够用阿里云提供的集中式用户身份管理和资源访问控制服务来管理其自身阿里云资源的访问权限。	未发现异常情况。
APD_10	客户未在阿里云官方网站上确认并同意服务条款前，其阿里云账户注册或产品购买订单将无法被处理，且所述服务条款中规定了与客户访问权限管理相关的责任和义务。	1. 询问了相应人员，以了解服务条款中规定客户访问权限管理责任和义务的情况，以及在阿里云官方网站上进行阿里云账户注册或产品购买期间客户确认接受相关条款的流程。 2. 检查了阿里云官方网站上服务条款的样本，以确认明确规定了与客户访问权限管理相关的责任和义务。 3. 检查了账户注册流程和产品购买流程，以确认如果客户未确认并同意阿里云官方网站上的服务条款，其账户注册流程和产品购买操作将无法处理。	未发现异常情况。
APD_11	Root 特权仅向授权人员提供。Root 账户密码每个月自动轮换一次。特权 sudo root 指令的使用将会	1. 询问了相应人员，以了解通过既定程序限制访问 root 特权的情况以及针对特权 sudo root 指令的	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	被记录并监控。	记录和监视情况。 2. 检查了访问管理系统的配置，以确认未向终端用户开放 root 账户访问权限的申请，且 root 账户密码每个月自动轮换。 3. 检查了日志集中管理平台和风险警报的样本，以确认记录并监控了 特权 sudo root 指令。	
APD_12	阿里云在访问监控系统中定义监控规则，以分析账户和权限的使用情况。根据监控结果系统自动生成预警，并由安全团队跟进。	1. 询问了相应人员，以了解针对用户账户和访问权限使用情况制定的监控流程。 2. 检查了访问监控系统的预警样本，以确认根据预定义的审核规则自动生成了预警，并由安全团队进行审查、后续跟进和记录。	未发现异常情况。
APD_13	阿里云制定了相关程序，以确保员工职位或所属部门变更时，会自动通知员工和员工的主管审核并归还不再需要的应用系统访问权限，并删除员工的物理服务器、网络设备和虚拟机访问权限。	1. 询问了相应人员，以了解员工职位或所属部门变更时，针对其所拥有的应用系统、物理服务器、网络设备和虚拟机的访问权限制定的管理流程。 2. 检查了发送通知的系统逻辑，以确认身份认证系统实时接收来自人力资源系统的员工信息和来自权限管理系统的权限分配信息，并且当员工职位或所属部门变更时，自动触发权限管理系统向员工和员工的主管发送访问权限调整的电子邮件通知。 3. 检查了权限管理系统向跨业务组转岗员工以及主管发送的访问权限调整电子邮件通知的样本，以确定在转岗发生时权限管理系统自动向员工及其主管发送访问权限调整的电子邮件通知。 4. 检查了删除访问权限的系统逻辑，以确认权限管理系统实时接收来自人力资源系统的员工信息，并且当员工职位或所属部门变更时，自动删除员	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		工的物理服务器、网络设备和虚拟机访问权限。 5. 检查了在人力资源系统抽取的转岗员工样本对应的权限删除记录，以确认其物理服务器、网络设备和虚拟机的访问权限已被禁用。	
APD_14	阿里云制定了自动禁用离职员工 Active Directory 账户的程序。	1. 询问了相应人员，以了解根据人力资源系统信息自动禁用离职员工 Active Directory 账户的程序。 2. 检查了禁用 Active Directory 账户的系统逻辑，以确认身份验证系统从人力资源系统实时接收员工信息，并自动禁用离职员工的 Active Directory 账户。 3. 检查了身份验证系统禁用人力资源系统中离职员工样本的 Active Directory 账户记录，以确认该离职员工的 Active Directory 账户在离职生效日即已在系统中自动禁用。	未发现异常情况。
APD_15	制定了自动禁用离职员工 Active Directory 账户的程序。	1. 询问了相应人员，以了解根据人力资源系统中的信息自动禁用离职员工 Active Directory 账户的程序。 2. 检查了禁用 Active Directory 账户的系统逻辑，以确认身份验证系统从人力资源系统接收实时员工信息，并自动禁用离职员工的 Active Directory 账户。 3. 检查了人力资源系统中一位选定离职员工在身份验证系统中的 Active Directory 账户禁用记录，以确认该离职员工的 Active Directory 账户在离职生效日即已在系统中自动禁用。	未发现异常情况。
APD_16	基础架构团队负责确保进行运维生产系统的操作只	1. 询问了相应人员，以了解通过堡垒主机限制访问	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	能通过堡垒机实现访问。并且需通过双因素认证方可访问堡垒机。	生产系统的程序以及访问堡垒主机的身份验证机制。 2. 检查了访问生产系统的流程，以确认用户须登录堡垒主机方可访问生产系统，并且需要通过双因素认证方可登录堡垒主机。	
APD_17	需经授权人员批准方可提供物理服务器、网络设备和虚拟机的访问权限。	1. 询问了相应人员，以了解申请和批准物理服务器、网络设备和虚拟机访问权限的程序。 2. 检查了物理服务器、网络设备和虚拟机访问权限样本的申请和批准情况，以确认需经授权人员批准后方可根据申请人的职位和角色相应提供此类访问权限，且申请人与批准人之间进行了严格的职责分离。	未发现异常情况。
APD_18	客户可通过管理控制台中的工单服务向阿里云员工提供访问该客户阿里云资源的外部临时访问权限。该访问权限仅限根据客户配置的授权设置相应提供。	1. 询问了相应人员，以了解客户向阿里云员工提供访问该客户资源的外部临时访问权限的程序和身份验证机制。 2. 检查了客户向阿里云员工提供外部临时访问权限的过程，以确认客户阿里云资源的访问权限需经客户批准后方提供，且仅限根据客户配置的授权设置提供此类访问权限。	未发现异常情况。
APD_19	通过堡垒机在生产系统中执行的所有活动均被实时记录并传送至日志集中管理平台。日志将保留至少半年，且用户无法对其进行修改或删除。	1. 询问了相应人员，以了解生产系统中活动的日志记录情况，以及日志的保留期限要求和保护措施。 2. 检查了日志记录的配置，以确认日志至少保留半年，且用户无法对其进行修改或删除。 3. 检查了服务器样本的日志，以确认记录了生产系统内的活动，且相应的日志在日志集中管理平台中保留。	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
APD_20	阿里云制定了监控规定，以对日志集中管理平台内的日志记录执行自动检查。根据审查结果自动生成预警并发送给安全团队进行调查。	1. 询问了相应人员，以了解针对日志集中管理平台中留存的生产系统日志记录制定的监控程序。 2. 检查了日志集中管理平台内的日志监控的系统逻辑，以确认制定了监控规定以审核活动日志并识别异常用户活动。 3. 检查了风险管理平台，以确认系统根据预定义的审核规则自动生成了预警并发送到平台供安全团队审查。	未发现异常情况。
APD_ECS_21	**适用于 ECS** 默认设置下，只有创建自定义镜像的用户可以访问及使用该镜像。仅当创建自定义镜像的用户将该镜像与其他阿里云账户共享后，其他阿里云账户才可对该自定义镜像进行访问。	1. 询问了相应人员，以了解阿里云对自创 ECS 实例镜像和共享镜像配置的 ECS 访问控制规则。 2. 检查了使用阿里云账户创建自定义 ECS 实例镜像的流程和访问权限，以确认在没有镜像创建账户授权的情况下另一阿里云账户无法访问该镜像。 3. 检查了镜像分享流程，以确认只有经授权的阿里云账户才可访问共享镜像。	未发现异常情况。
APD_IoT_22	**适用于物联网平台** 阿里云物联网平台用日志管理平台记录操作系统、服务器和网络设备内的用户操作。日志不可修改，且至少保留 30 天。	1. 询问了相应人员，以了解阿里云物联网平台目前用于记录相关服务器和网络设备上生成的操作日志的日志管理平台。 2. 检查了日志管理平台，以确认操作日志相应在平台内记录。 3. 检查了存储在日志管理平台中日志的访问配置，以确认仅向员工提供只读权限。 4. 检查了存储在日志管理平台中日志的保留期配置，以确保日志至少保留 30 天。	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
APD_IoT_23	适用于物联网平台 阿里云物联网平台已在日志服务系统中建立了日志保留机制，以确保过期日志记录自动从系统中删除。	1. 询问了相应人员，以了解阿里云物联网平台的日志保留策略。 2. 观察了物联网平台工程师所展示的生产环境中阿里云物联网平台采用的日志保留策略，以确认系统内正确定义和配置了相关的日志保留策略。 3. 观察到物联网平台工程师所展示的后端日志管理系统维护的日志记录，以确认阿里云物联网平台维护了 30 天的日志，并且超过 30 天的日志会自动删除。	未发现异常情况。
APD_IoT_24	适用于物联网平台 各项物联网设备均分配了 productKey 和 deviceName 的唯一组合，以确保设备标识的唯一性。	1. 询问了适当人员，以了解阿里云物联网平台用于确保设备标识唯一性的机制，即各项物联网设备均分配了 productKey 和 deviceName 的唯一组合以确保唯一性。 2. 检查了产品相关的数据库表的结构，以确认使用了 productKey 和 deviceName 的唯一组合来定义主键，以确保设备的唯一性。	未发现异常情况。
APD_IoT_25	适用于物联网平台 阿里云物联网平台使用的签名验证机制通过 productKey、deviceName 和 deviceSecret 来验证设备的身份。	1. 询问了相应人员，以了解阿里云物联网平台的签名验证机制。 2. 检查了阿里云物联网平台所采用的签名验证算法，以确认提供了三种签名验证机制。 3. 创建一组身份信息（productKey、deviceName、deviceSecret），并使用正确的信息测试需要签名的身份验证机制，以确认使用正确的信息时身份验证成功。 4. 分别修改 productKey、deviceName 和 deviceSecret，并使用初始信息测试需要签名的	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		身份验证机制，以确认使用错误信息时身份验证失败。	
APD_IoT_26	适用于物联网平台 客户可通过管理控制台删除物联网设备。删除后不能重新激活设备，因为设备的相关 productKey、deviceName、deviceSecret 均已废弃。	1. 询问了相应人员，以了解阿里云物联网平台的设备删除机制。 2. 观察了物联网平台工程师创建一套身份信息（productKey、deviceName、deviceSecret），并测试要求签名的身份验证机制，以确认使用正确信息时可成功实现身份验证。 3. 观察了物联网平台工程师删除设备相关身份信息（productKey、deviceName、deviceSecret），并尝试使用这些初始信息重新进行身份验证，以确认身份验证失败。	未发现异常情况。
APD_IoT_27	适用于物联网平台 阿里云物联网平台为客户升级固件所创建的 URL 仅在 24 小时内有效。过期的 URL 无法用来升级固件。	1. 询问了相应人员，以了解阿里云物联网平台的固件升级机制。 2. 观察了物联网平台工程师将新固件包上传到管理控制台并生成用于固件升级的 URL 链接，随后在 24 小时内下载了该新固件包，以确认下载请求成功。 3. 观察了物联网平台工程师在 24 小时后上传带有原始 URL 链接的新固件包，以确认下载请求失败并显示该链接已过期。	未发现异常情况。
APD_IoT_28	适用于物联网平台 阿里云物联网平台采用阿里云 KMS 服务来分发密钥以确保保密性。	1. 询问了相应人员，以了解阿里云物联网平台的密钥管理机制，发现物联网平台使用 KMS 来分发密钥。 2. 检查了 KMS 中的加密算法和密钥配置，以确认阿里云物联网平台采用 KMS。	未发现异常情况。

控制目标 3: 程序和数据访问			
控制合理保证了每个系统模块的逻辑访问权限仅限于相应人员，以防止越权访问，并对用户的异常活动进行监控。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 检查了用于在阿里云物联网平台内调用 KMS 接口的代码配置，以确认物联网平台使用 KMS 来分发密钥以确保保密性。	

控制目标 4: 数据安全			
控制合理保证了数据的完整性、准确性和安全性可在传输、存储和处理过程中得到维护。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
DSI_01	阿里巴巴集团制定了《数据安全规范》，旨在定义不同的数据类型、数据所有者、数据分类标准、数据安全等级和保护措施。该政策还规范了数据安全管理生命周期，包括数据生成、数据存储、数据使用、数据传输、数据分发和数据销毁。	1. 询问了相应人员，以了解阿里云用于管理数据分类、数据安全等级、数据保护措施和数据安全管理生命周期的数据安全规范，以及每年审查数据安全规范的流程。 2. 检查了数据安全管理文档，以确认已制定相关政策和程序，用以确保根据既定标准在数据管理生命周期内全程保护数据。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次数据安全规范。	未发现异常情况。
DSI_02	阿里云建立了数据安全平台以维护数据，包括保留期、分类和安全等级相关的信息。 尝试变更数据分类时会触发审批。	1. 询问了相应人员，以了解数据安全平台的数据维护流程，以及数据分类变更的申请和审批流程。 2. 检查了数据安全平台上数据分类变更的审批机制，以确认尝试变更数据分类时会基于预定义的审批工作流程触发适当等级的审批。	未发现异常情况。
DSI_03	在硬盘驱动器被转移出数据中心或释放空间以备重用之前，阿里云采取了数据安全擦除流程。	1. 询问了相应人员，以了解硬盘驱动器被转移出数据中心或释放空间以备重用之前的数据安全擦除流程。 2. 检查了数据覆盖机制，以确认硬盘驱动器上的数据经过数次覆盖，并且进行了验证检查，以	未发现异常情况。

控制目标 4: 数据安全			
控制合理保证了数据的完整性、准确性和安全性可在传输、存储和处理过程中得到维护。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		确保成功完成驱动器的完全覆盖。 3. 检查了数据安全擦除日志，以确认硬盘驱动器被转移出数据中心或释放空间以备重用，之前上面的数据经过数次覆盖。	
DSI_04	硬盘驱动器在被报废处置之前按照数据安全规范销毁。	1. 询问了相应人员，以了解硬盘驱动器销毁的流程，使其保存的数据在销毁前无法读取。 2. 检查了硬盘驱动器处理请求样本，以确认硬盘驱动器在被报废处置之前按照数据安全规范销毁。	未发现异常情况。
DSI_05	阿里云制定了《阿里云信息传输安全管理规定》，明确数据传输的安全管理要求和措施。	1. 询问了相应人员，以了解阿里云执行既定数据传输安全管理程序以管理安全要求和数据传输方法的情况，以及每年审查数据传输安全程序的流程。 2. 检查了数据传输安全管理文档，以确认制定了相关政策和程序以确保根据一致的标准安全地传输所有数据。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次数据传输安全管理政策。	未发现异常情况。
DSI_06	当阿里云与客户之间的服务协议到期时，系统在数据保留期限到期时释放客户的实例后，客户数据会根据相关协议自动被清除。	1. 询问了相应人员，以了解系统的自动数据擦除机制。数据保留期满时，客户数据（包括元数据）会被清除。 2. 检查了客户数据擦除记录，以确认阿里云在数据保留期满时自动释放并清除客户数据（包括元数据）。	未发现异常情况。
DSI_ECS_07	**适用于 ECS** ECS 使用安全的通信渠道供客户远程登录。	1. 询问了相应人员，以了解阿里云 ECS 产品通过为客户创建安全隧道远程连接到 Windows 和	未发现异常情况。

控制目标 4: 数据安全			
控制合理保证了数据的完整性、准确性和安全性可在传输、存储和处理过程中得到维护。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		Linux 系统上建立的 ECS 实例远程连接功能。 2. 检查了使用 VNC 和 Windows 远程桌面连接远程连接到 Windows 实例的过程，以确认建立了安全连接隧道。 3. 检查了使用 VNC 和 SSH 密钥对远程连接到 Linux 实例的过程，以确认建立了安全连接隧道。	
DSI_OSS_08	**适用于 OSS** OSS 支持从服务器端通过 MD5 哈希字符串对客户数据进行完整性验证。	1. 询问了相应人员，以了解 OSS 从服务器端对客户上传数据通过 MD5 哈希字符串进行完整性验证的功能。 2. 执行了完整性验证测试，以确认 OSS 服务器会拒绝含不同 MD5 值文件的上传请求。	未发现异常情况。
DSI_ECS_OSS_RDS_09	**适用于 ECS、OSS 和 RDS** 阿里云在官方网站上发布了 ECS、OSS 和 RDS 相关的用户产品文档，其中规定了有关客户数据保留的政策。	1. 询问了相应人员，以了解阿里云官方网站上发布的 ECS、OSS 和 RDS 用户产品文档中规定的有关客户数据保留的政策。 2. 检查了阿里云官方网站上发布的与 ECS、OSS 和 RDS 相关的用户产品文档，以确认制定了数据保留政策以阐明相关责任。	未发现异常情况。
DSI_VPN_10	**适用于 VPN 网关** 阿里云 VPN 网关支持 以 AES 256 和 IKEv1/IKEv2 算法为基础的数据加密传输机制，以确保 VPC 与本地数据中心之间或 VPC 与客户端之间的数据传输安全性。	1. 询问了相应人员，以了解 VPN 网关产品支持的以 AES 256 和 IKEv1/IKEv2 算法为基础的数据加密传输机制，以确保 VPC 网络与本地数据中心之间或 VPC 与客户端之间的数据传输安全性。 2. 检查了从管理控制台创建 SSL 服务器的页面，以确认 VPN 网关支持客户选择 AES 256 算法。	未发现异常情况。

控制目标 4: 数据安全			
控制合理保证了数据的完整性、准确性和安全性可在传输、存储和处理过程中得到维护。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 检查了从管理控制台创建 IPSec 服务器的页面，以确认 VPN 网关支持客户选择 IKEv1/IKEv2 算法。	
DSI_VPN_11	**适用于 VPN 网关** 阿里云 VPN 网关启用了身份验证机制。客户端通过 VPN SSL 功能连接到 VPC 之前需要对客户端上的证书进行身份验证。	1. 询问了相应人员，以了解在建立基于 VPN SSL 的通信线路之前验证 VPN 网关产品证书的信息。 2. 检查了在管理控制台上创建基于 SSL 的 VPN 网关服务器的过程，以确认使用经核实的身份证书可连接成功。 3. 检查了使用修改后的客户端证书连接到 VPN 网关服务器客户端的过程，以确认用错误身份证书无法建立连接。	未发现异常情况。
DSI_IoT_12	**适用于物联网平台** 阿里云物联网平台通过阿里云官方网站发布相关的 SDK 软件包和 API 接口。	1. 询问了相应人员，以了解阿里云物联网官方网站上 SDK 软件包和 API 接口的发布机制。 2. 检查了物联网平台中的 SDK 下载页面，以确认 SDK 软件包通过阿里云物联网官方网站发布。 3. 检查了物联网平台中的 API 接口页面，以确认产品相关的 API 接口通过阿里云的物联网官方网站发布。 4.	未发现异常情况。
DSI_IoT_13	**适用于物联网平台** 阿里云物联网平台采用 HTTPS 协议，以保障客户执行固件升级流程的安全性。	1. 询问了相应人员，以了解阿里云物联网平台固件升级流程中采用的协议。 2. 执行了基于阿里云物联网平台的固件包下载测试。通过对固件包下载过程中的流量进行分析，确认使用了 HTTPS 协议来确保数据传输的安全性。	未发现异常情况。
DSI_IoT_14	**适用于物联网平台**	1. 询问了相应人员，以了解阿里云物联网平台采	未发现异常情况。

控制目标 4: 数据安全			
控制合理保证了数据的完整性、准确性和安全性可在传输、存储和处理过程中得到维护。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	阿里云物联网平台启用了基于 MD5 技术的完整性校验机制，以保证设备从云服务器下载的固件包未经过篡改。	用的 MD5 技术，以确认从云服务器下载到设备期间固件包未经过篡改。 2. 执行了请求升级固件的测试，观察了固件升级期间物联网平台工程师生成相关日志记录，以确认存在 MD5 值对比流程，即根据接收的固件包获得计算出的 MD5 值，并将该值与从客户端接收的 MD5 值进行对比。最后检查了相关记录，以确认当 MD5 值相同时，升级请求成功，当 MD5 值不同时，升级请求失败。	
DSI_IoT_15	适用于物联网平台 当客户注销阿里云服务账户时，阿里云物联网平台会在账户注销 18 个月后完成对所有产品相关数据的物理删除。	1. 询问了相应人员，以了解阿里云物联网平台的账户数据删除机制。 2. 检查了阿里云物联网平台的逻辑数据删除脚本和数据删除日志，以确认租户的账号删除后，系统会标记租户的产品相关数据以实现逻辑数据删除。 3. 检查了租户的账号删除后系统定义的数据保留策略，以确认这些数据只能保留指定天数。 4. 检查了物理数据删除机制的脚本，以确认系统会调用物理数据删除接口，以确保在数据保留期结束后，该服务账号相关的所有数据都能被删除。	未发现异常情况。
DSI_IoT_16	适用于物联网平台 当通过相关 API 使用 MQTT 或 HTTP 协议时，阿里云物联网平台采用 TLS 来确保云服务器与设备/网关之间数据传输的安全性，而当使用 CoAP 协议时，采用 DTLS 来确保设备/网关到云服务器之间建立安全的数据传输。	1. 询问了相应人员，以了解阿里云物联网平台采用的安全传输机制。 2. 执行了在阿里云物联网平台内通过 API 接口基于 MQTT 或 HTTP 协议建立设备/网关侧到云平台的传输通道的测试。然后执行了流量分析，以确认使用了 TLS 加密协议来确保传输数据经过加密。	未发现异常情况。

控制目标 4: 数据安全			
控制合理保证了数据的完整性、准确性和安全性可在传输、存储和处理过程中得到维护。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 执行了在阿里云物联网平台内基于 CoAP 协议建立设备/网关侧到云平台的传输通道的测试。然后执行了流量分析，以确认使用了 DTLS 加密协议来确保传输数据经过加密。	
EKM_01	阿里云制定了《阿里云密码和密钥管理规定》，旨在规范密钥的生成、存储、使用、分配、备份、恢复、更换和销毁。	1. 询问了相应人员，以了解阿里云规范密钥管理流程的政策，以及每年审查相关政策的流程。 2. 检查了密钥管理文档，以确认阿里云制定了正式的政策和程序，用以确保根据既定标准在密钥的生成、存储、使用、分配、备份、恢复、更换和销毁期间保护密钥。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次密钥管理政策并在必要时更新。	未发现异常情况。
EKM_04	阿里云控制台使用 HTTPS 加密进行 ECS 和密钥管理服务的数据传输。当客户登录控制台并执行操作时，通过 HTTPS 发送身份验证信息和操作命令。当客户使用控制台上“连接到管理终端”中的 VPC 来管理 ECS 实例时会实施 HTTPS 连接。密钥管理服务的 API 请求须通过 HTTPS 进行 。	1. 询问了相应人员,以了解数据传输中使用的安全协议。 2. 检查了管理控制台登录和操作请求流程，以确认 ECS 和密钥管理服务的身份验证信息和操作请求通过 HTTPS 协议传输。 3. 检查了 ECS 远程连接流程，以确认使用 VPC 连接到管理终端时受到 HTTPS 保护。 4. 检查了 API 请求流程，以确认密钥管理服务的用户请求须通过 HTTPS 进行。	未发现异常情况。
EKM_05	阿里云使用行业标准的 256 位密钥长度的 TLS 协议（如适用）进行数据传输。客户可以选择不同版本的 TLS 协议。	1. 询问了相应人员,以了解数据传输中使用的安全协议。 2. 检查了管理控制台和数据传输流程，以确认使	未发现异常情况。

控制目标 4: 数据安全			
控制合理保证了数据的完整性、准确性和安全性可在传输、存储和处理过程中得到维护。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		用行业标准的 256 位密钥长度的 TLS 协议（如适用）进行数据传输，且客户可以选择不同版本的 TLS 协议。	
EKM_06	阿里云支持 256 位密钥长度的高级加密标准，以对静态数据进行加密。客户可以使用阿里云密钥管理服务创建或上传用户自选密钥，管理密钥轮换和保护等级，并对存储在阿里云服务中的数据进行加密。	1. 询问了相应人员,以了解用于加密存储数据的安全协议。 2. 检查了管理控制台和和数据存储加密配置的流程，以确认客户可以使用 256 位密钥长度的高级加密标准或通过使用阿里云密钥管理服务对其数据进行加密。 3. 检查了密钥管理服务，以确认客户可以创建或上传用户自选密钥，管理密钥轮换和保护等级，并对存储在阿里云服务中的数据进行加密。	未发现异常情况。
EKM_OSS_RDS_07	**适用于 OSS 和 RDS** 部分版本的阿里云 RDS 实例（在具有本地 SSD 的高可用性版 RDS 上运行的 MySQL 8.0 版、在具有本地 SSD 的高可用性版 RDS 运行的 MySQL 5.7 版和 MySQL 5.6 版）支持透明数据加密。阿里云 OSS 支持服务器端加密。	1. 询问了相应人员,以了解 RDS 和 OSS 的存储加密功能。 2. 检查了 RDS 和 OSS 的存储加密功能，以确认某些版本的 RDS 实例提供了透明数据加密功能，并且 OSS 支持使用基于 256 位密钥长度的高级加密标准或使用密钥管理服务中管理的用户自选密钥进行服务器端加密。	未发现异常情况。
EKM_IoT_08	**适用于物联网平台** 阿里云物联网平台采用加密存储机制，以保障 deviceSecret 的安全。	1. 询问了相应人员，以了解阿里云物联网平台采用的加密存储机制。 2. 检查了数据库中存储加密相关的代码，以确认阿里云物联网平台已采用加密机制。 3. 执行了测试以在管理控制台中创建 deviceSecret，然后通过阿里云物联网平台的后端数据库系统检查了该 deviceSecret 的状态，	未发现异常情况。

控制目标 4: 数据安全			
控制合理保证了数据的完整性、准确性和安全性可在传输、存储和处理过程中得到维护。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		以确认 deviceSecret 采用了数据加密机制。	
EKM_KMS_09	适用于密钥管理服务 阿里云密钥管理服务的硬件安全模块（HSM）已通过验证和认证。	1. 询问了相应人员,以了解 HSM 的认证情况。 2. 检查了阿里云持有的 HSM 国际和本地认证，以确定阿里云所有的 HSM 已通过验证和认证。	未发现异常情况。
EKM_KMS_10	适用于密钥管理服务 阿里云密钥管理服务（KMS）使用阿里云资源访问管理（RAM） 进行身份验证和访问权限管理。	1. 询问了相应人员，以了解 KMS 的访问控制机制。 2. 检查了对子账号未分配任何权限权限的流程，以确认此类子账号不能访问 KMS 服务。 3. 检查了对子账号分配只读权限的流程，以确认此类子账号能够成功访问 KMS 服务。	未发现异常情况。
IPY_01	阿里云 API 网关支持对 API 请求进行基于 HTTPS 的加密。在管理控制台有不同的 HTTPS 安全政策可供选择。	1. 询问了相应人员，以了解管理控制台中 API 网关支持的协议和安全策略。 2. 检查了在管理控制台中配置 API 操作的流程，并确认 API 网关支持对 API 请求进行基于 HTTPS 的加密并有不同的 HTTPS 安全政策可供选择。	未发现异常情况。

控制目标 5: 程序变更管理			
控制合理保证了每个系统模块的变更请求将经过测试和验证，以防止未经授权的修改。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
CCC_01	阿里云制定了《阿里云软件开发安全管理规定》，以规范软件开发过程中的安全标准，包括需求分析、系统设计、安全代码、测试和发布，以减少安全漏洞。	1. 询问了相应人员，以了解阿里云制定相关政策以规范软件开发过程中的安全标准，以及审查相关政策和程序的流程。 2. 检查了相关政策的记录，以确认制定了正式的政	未发现异常情况。

控制目标 5: 程序变更管理			
控制合理保证了每个系统模块的变更请求将经过测试和验证，以防止未经授权的修改。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		策和程序以规范软件开发过程中的安全标准。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次相关政策，且必要时根据审查结果更新政策。	
CCC_02	阿里云制定了《阿里云新产品开服指引》，以规范从产品启动、安全架构审查、安全开发、安全验证、产品发布到事件响应的整个产品开发生命周期中的安全要求。	1. 询问了相应人员，以了解阿里云制定相关政策以明确针对整个产品开发生命周期的制定的安全要求，以及每年审查相关政策和程序的流程。 2. 检查了相关政策的记录，以确认制定了正式的政策和程序以规范产品开发生命周期中的安全要求。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次相关政策，且必要时根据审查结果更新政策。	未发现异常情况。
CCC_03	阿里巴巴集团制定了《阿里巴巴变更管理规范》，以规范生产中所有可能影响业务运营的变更操作。所有对生产系统的操作均须记录在变更管理平台上，并遵照标准要求进行变更的设计、开发、测试、批准、发布和回滚。	1. 询问了相应的人员，以了解阿里云制定相关政策并要求记录生产中所有可能影响业务运营的变更操作并遵循标准管理程序的情况，以及每年审查相关政策和程序的流程。 2. 检查了相关政策的文档，以确认制定了正式的政策和程序以规范生产中所有可能影响业务运营的变更操作。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次相关政策，且必要时根据审查结果更新政策。	未发现异常情况。
CCC_04	公共云及金融云的变更操作均遵循《公共云变更管理规范》。对云平台的所有变更均须根据变更管理标准加以记录、评估、测试、批准和实施。	1. 询问了相应人员，以了解阿里云制定相关政策以规范对公共云和金融云的变更流程，以及每年审查相关政策和程序的流程。	未发现异常情况。

控制目标 5: 程序变更管理			
控制合理保证了每个系统模块的变更请求将经过测试和验证，以防止未经授权的修改。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		2. 检查了相关政策的文档，以确认制定了正式的政策和程序以规范与云运营相关的变更操作。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次相关政策，且必要时根据审查结果更新政策。	
CCC_05	阿里云制定了《阿里云信息技术服务配置与资产管理规定》，以规范配置变更管理流程。所有配置变更均须在部署前进行评估、测试和授权。	1. 询问了相应人员，以了解阿里云制定相关政策以管理配置变更管理流程的情况，以及每年审查相关政策和程序的流程。 2. 检查了相关政策的文档，以确认制定了正式的政策和程序以管理配置变更管理流程。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次相关政策，且必要时根据审查结果更新政策。	未发现异常情况。
CCC_06	阿里云建立了多种与客户沟通的渠道，以向内外部用户通知可能对其产生影响的阿里云产品、系统元数据、配套基础设施和网络的变更。	1. 询问了相应人员，以了解向内外部用户通知可能对其产生影响的阿里云产品、系统元数据、配套基础架构和网络变更的程序。 2. 检查了阿里云产品、系统元数据、配套基础设施和网络变更样本的变更需求和通知消息，以确认向预期会受到影响的用户通知了该变更。	未发现异常情况。
CCC_07	在将阿里云产品、配套基础设施和网络的变更部署到生产环境之前，代码审核人对源代码变更执行代码审核。	1. 询问了相应人员，以了解变更部署之前执行代码审核的要求和流程。 2. 检查了部署到到生产环境的源代码变更样本以及相关变更需求和代码审核的支持性证据，以确认基于已建立的标准执行了代码审核，以及确保代码开发者与代码审核者已建立职责分离。	未发现异常情况。
CCC_08	在将阿里云产品、系统元数据、配套基础设施和	1. 询问了相应人员，以了解将阿里云产品、系统元	未发现异常情况。

控制目标 5: 程序变更管理			
控制合理保证了每个系统模块的变更请求将经过测试和验证，以防止未经授权的修改。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	网络的变更部署到生产环境之前，变更需求由授权人员审核并批准。	数据、配套基础设施和网络的变更部署到生产环境之前对变更需求的审核和批准流程。 2. 检查了阿里云产品、系统元数据、配套基础设施和网络变更样本的变更需求和批准记录，以确认在变更部署到生产环境之前获得授权人员的批准，以及确保请求者和批准者已建立职责分离。	
CCC_09	在将阿里云产品、配套基础设施和网络的变更部署到生产环境之前，变更须经过测试，并确保测试结果被记录。	1. 询问了相应人员，以了解将阿里云产品、配套基础设施和网络的变更部署到生产环境之前对变更执行测试以及记录测试结果的流程。 2. 检查了阿里云产品、配套基础设施和网络的变更样本的变更需求和测试记录，以确认在部署之前变更经过测试，并记录了测试结果。	未发现异常情况。
CCC_10	在将阿里云产品、配套基础设施和网络的变更部署到生产环境之前，须制定回滚方案。	1. 询问了相应人员，以了解将阿里云产品、配套基础设施和网络的变更部署到生产环境之前制定和记录回滚方案的流程。 2. 检查了阿里云产品、配套基础设施和网络变更样本的变更需求和回滚方案，以确认在部署变更之前，制定和记录了将系统恢复变更前状态的回滚方案。	未发现异常情况。
CCC_11	在阿里云产品、系统元数据、配套基础设施和网络的变更流程中，须确保变更需求、批准和部署职责的分离。	1. 询问了相应人员，以了解阿里云产品、系统元数据、配套基础设施和网络变更请求、批准和实施等关键职责的分离流程。 2. 检查了阿里云产品、系统元数据、配套基础设施和网络变更样本的关键责任人，以确认执行了变更需求、批准和部署的职责分离。	未发现异常情况。
CCC_12	开发环境、测试环境和生产环境相互隔离。	1. 询问了相应人员，以了解执行既定程序以确保范围内阿里云产品的开发环境、测试环境和生产环	未发现异常情况。

控制目标 5: 程序变更管理			
控制合理保证了每个系统模块的变更请求将经过测试和验证，以防止未经授权的修改。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		境相互隔离的情况。 2. 检查了测试环境、开发环境和生产的网络隔离机制，以确认不同环境相互隔离。	

控制目标 6: 个人终端安全			
控制合理保证了阻止或检测引入未授权软件或恶意软件的操作。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
MOS_01	阿里云制定了《数据安全执行指南》，以指明授权的软件下载渠道和禁止在 PC 端使用的软件。	1. 询问了相应人员，以了解 PC 端软件安装的管理要求，以及每年审查相关政策和程序的流程。 2. 检查了《数据安全执行指南》，以确认阿里云制定了正式的政策，包括使用高风险软件和产品的相关规定，以规范授权的软件下载渠道和禁止在 PC 端使用的软件。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次《数据安全执行指南》。	未发现异常情况。
MOS_02	阿里云在员工的计算机上安装了阿里云终端管理软件，用于管控软件安装，并在该软件内备存授权软件列表。	1. 询问了相应人员，以了解有关在员工的计算机上安装和使用软件的限制。 2. 检查了阿里云的终端管理软件，以确认在软件内备存了授权软件列表。	未发现异常情况。
MOS_03	移动设备在连接到阿里云的 OA 子网之前，必须安装和启动阿里云的终端管理系统，以使该移动设备受到网络准入管理和终端保护。	1. 询问了相应人员，以了解与阿里云 OA 子网相连接的移动设备受限情况。 2. 检查了阿里巴巴员工登录员工移动设备的流程，尝试在没有登录终端管理软件的情况下将其移动设备连接阿里云的 OA 子网，以确认移动设备在连接到阿里云的 OA 子网之前必须安装并登录终端管理系统。	未发现异常情况。

控制目标 6: 个人终端安全			
控制合理保证了阻止或检测引入未授权软件或恶意软件的操作。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 检查了阿里巴巴员工登录终端管理软件的流程，以确认终端管理软件被用于管理网络准入和保护终端。 4. 检查了终端代理配置，以确认移动设备在连接到阿里云的 OA 子网之前，必须安装并启动终端管理软件。	
MOS_04	所有计算机分发给员工之前都会安装一个包含防病毒软件的标准镜像。防病毒软件可启动实时防护，每 4 小时更新一次病毒库，以及每周进行病毒扫描。	1. 询问了相应人员，以了解将带有预装防病毒软件的镜像部署到员工计算机的流程。 2. 检查了防病毒软件，以确认该软件启动实时防护，每 4 小时更新一次病毒库，且每周进行病毒扫描。	未发现异常情况。
MOS_05	员工无法执行关闭防病毒软件功能的操作。卸载员工计算机上的防病毒软件需要使用由 IT 部门统一管理的密码。	1. 询问了相应人员，以了解对阿里云员工计算机上停用防病毒软件操作的管控情况。 2. 检查了防病毒软件，并试图卸载该防病毒软件，以确认阿里云员工卸载防病毒软件时需要输入密码。 3. 检查了防病毒软件，并试图停用或关闭该防病毒软件，以确认阿里云员工无法执行停用防病毒软件功能的操作。	未发现异常情况。
MOS_06	阿里云在员工的计算机上安装数据泄露防护（DLP）软件，以检测在这些计算机上进行的敏感操作。阿里云的终端管理系统监控 DLP 软件的安装状况，如发现计算机未配备 DLP 软件，系统自动将 DLP 软件推送到计算机上安装。DLP 软件收集的敏感活动信息通过 DLP 监控平台根据预先设定的规则进行监控。根据监控自动结果生成警报，并由安全团队跟进。	1. 询问了相应人员，以了解针对员工在计算机上进行的敏感操作的监控措施。 2. 检查了相关配置，以确认员工计算机上的 DLP 软件安装受到监控，并且阿里云的终端管理软件会自动将 DLP 软件推送到未安装 DLP 的计算机上安装。 3. 检查了 DLP 收集的敏感活动样本，以确认是否对其进行了监控并恰当的进行后续跟进。	未发现异常情况。

控制目标 6: 个人终端安全			
控制合理保证了阻止或检测引入未授权软件或恶意软件的操作。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
MOS_07	所有计算机在分发给员工之前都会安装一个包含硬盘加密软件的标准镜像，员工无法卸载硬盘加密软件。	1. 询问了相应人员，以了解讲带有预安装硬盘加密软件的镜像部署到员工计算机的流程，以及对阿里云员工计算机设备上禁用硬盘加密软件操作的管控情况。 2. 检查了硬盘加密软件，以确认员工计算机硬盘上的数据由该加密软件进行保护。 3. 检查了硬盘加密软件，并试图卸载硬盘加密软件，以确认阿里云员工无权限卸载硬盘加密软件。	未发现异常情况。
TVM_03	阿里云制定了《阿里巴巴集团终端安全管理规定》，旨在规范用户终端设备上防病毒软件安装、授权软件安装和补丁更新的程序。	1. 询问了相应人员，以了解《阿里巴巴集团终端安全管理规定》中规范的用户终端设备防病毒软件安装、授权软件安装和补丁更新管理流程，以及每年审核终端安全管理规定的流程。 2. 检查了《阿里巴巴集团终端安全管理规定》，以确认阿里云制定了正式政策来规范在用户终端设备上安装防病毒软件、安装授权软件和更新补丁的流程，并且至少每年对该政策进行审核。	未发现异常情况。

控制目标 7: 物理安全和环境管理			
控制合理保证了对硬件和存储介质的物理访问仅限于授权人员，并且实施了相应的物理环境控制。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
DCS_01	阿里云制定了《阿里云物理和环境安全管理规定》，以根据最小特权原则规范内部和外部人员访问的管理和数据中心环境控制的要求。	1. 询问了相应人员，以了解根据《阿里云物理和环境安全管理规定》规范访问管理和安全边界措施的情况，以及每年审查访问和环境管理政策的流程。 2. 检查了有关数据中心物理和环境安全管理文档，以确认制定了政策和程序用以指导员工实施数据中心的访问管理和安全边界的保护措施。	未发现异常情况。

控制目标 7: 物理安全和环境管理			
控制合理保证了对硬件和存储介质的物理访问仅限于授权人员，并且实施了相应的物理环境控制。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次数据中心的物理和环境安全管理政策和程序。	
DCS_02	阿里云与数据中心服务提供商签订了合同和服务协议，其中规定了阿里云的信息安全责任和义务以及数据中心服务的可用性等级和服务范围。	1. 询问了相应人员，以了解阿里云和数据中心服务提供商在信息安全方面的责任和义务、门户的设计方式以及是否协定了计划内外审计的权利。 2. 检查了阿里云与选定数据中心服务提供商签订的合同，以确认是否明确规定了阿里云和数据中心服务提供商（包括分包商）在信息安全方面的责任和义务以及是否包含相关的法律和监管要求以及事件和漏洞管理要求。 3. 检查了阿里云与选定数据中心服务提供商签订的 服务等级协定（SLA），以确认 SLA 中明确规定了阿里云的要求及服务范围。	未发现异常情况。
DCS_03	数据中心经理须向数据中心服务提供商的人员通知数据中心访问权限的提供、修改和终止。	1. 询问了相应人员，以了解向数据中心服务提供商通知数据中心访问权限的提供、修改和终止的程序。 2. 检查了数据中心经理提供的审批和通知记录，以确认数据中心经理必须向数据中心服务提供商通知数据中心访问权限的提供、修改和终止的情况。	未发现异常情况。
DCS_04	经数据中心经理授权并向数据中心服务提供商的人员通知了访客的身份后访客方可进入数据中心和服务器机房区域。	1. 询问了相应人员，以了解数据中心的访客授权程序。 2. 检查了数据中心经理提供的授权和通知记录，以确认向数据中心服务提供商通知了访客的身份且数据中心经理已经通过 IDC 系统批准了此次访问。	未发现异常情况。

控制目标 7: 物理安全和环境管理			
控制合理保证了对硬件和存储介质的物理访问仅限于授权人员，并且实施了相应的物理环境控制。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
DCS_05	访客和外部供应商出入服务器机房必须由授权人员陪同。访问情况将被记录。	1. 询问了相应人员，以了解数据中心的访客访问的管理流程。 2. 检查了访客日志样本，以确认访客和外部供应商出入服务器机房由授权人员陪同且访问情况将被记录。	未发现异常情况。
DCS_06	阿里云数据中心已在数据中心入口处、设备交付区和所有关键访问点安装视频监控。录像要求至少保存三个月。此外，阿里云数据中心的值班人员 24/7 全天候监控数据中心的运行。	1. 询问了相应人员，以了解数据中心监控室的视频监控、录像保留期和人员职责。 2. 检查了数据中心样本中的闭路电视摄像机，以确认已在数据中心和服务器机房的入口处、设备交付区及所有关键访问点安装视频监控。 3. 检查了闭路电视录像样本，以确认录像至少保存三个月。 4. 检查了数据中心样本中的值班记录，以确认数据中心 24/7 全天候配备阿里云值班人员。	未发现异常情况。
DCS_07	只有被授权的人员才可以获取数据中心的出入权限。适当的人员每月对具有数据中心访问权限的用户进行权限审核。	1. 询问了相应人员，以了解定期进行数据中心访问权限审核的程序。 2. 检查了数据中心访问权限的审核记录样本，以确认适当人员每月对数据中心访问权限进行审核。	未发现异常情况。
DCS_08	数据中心设置了环境控制措施，包括机房的暖通空调、避雷系统、火灾探测和灭火系统、电源管理系统及监测温度和湿度的传感器。	1. 询问了相应人员，以了解数据中心设置的环境控制措施。 2. 观察了数据中心样本，以确认数据中心设置了环境控制措施，包括机房的暖通空调、避雷系统、火灾探测和灭火系统、电源管理系统及监测温度和湿度的传感器。	未发现异常情况。

控制目标 7: 物理安全和环境管理			
控制合理保证了对硬件和存储介质的物理访问仅限于授权人员，并且实施了相应的物理环境控制。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
DCS_09	阿里云使用设备监控系统对数据中心环境和服务器性能进行监控。如有异常，系统会自动触发警报，且现场操作员会与数据中心服务提供商跟进以解决问题。	1. 询问了相应人员，以了解数据中心环境和服务器性能的监控情况以及出现异常时的警报系统。 2. 检查了设备监控系统中的警报记录样本，以确认在出现性能异常时是否以及如何自动触发警报，并由现场操作员与数据中心服务提供商跟进以解决问题。	未发现异常情况。
DCS_10	阿里云为数据中心部署了网络设备的双路供电和双机热备。不间断电源（UPS）和内部柴油发电机已安装在数据中心，以便在出现电气故障时提供备用支持。	1. 询问了相应人员，以了解在数据中心部署的网络设备双路供电和双机热备的情况。 2. 检查了数据中心的电源设备、电路图、网络设备监控系统和网络拓扑结构，以确认为数据中心部署了网络设备的双路供电和双机热备，并在数据中心安装了不间断电源 (UPS) 和内部柴油发电机。	未发现异常情况。
DCS_11	数据中心访问权限由读卡器、生物特征识别机制、或物理锁来控制。	1. 询问了相应人员，以了解在数据中心实施的物理访问机制。 2. 观察了数据中心样本，以确认数据中心设置了读卡器、生物特征识别机制、或物理锁来控制权限访问。	未发现异常情况。
DCS_12	数据中心用于存储信息技术设备和系统的服务器机房区与办公区和运输区分隔开来。	1. 询问了相应人员，以了解数据中心中服务器机房区与办公区和运输区的物理隔离机制。 2. 观察了数据中心样本，以确认数据中心设置了相互隔离的用于存储信息技术设备和系统的服务器机房区与办公区和运输区。	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
BCR_01	阿里云制定了《阿里云业务连续性管理政策》和《阿里云信息技术管理体系手册》，以规范业务连续性管理。该政策定义了相关方的角色和职责、业务连续性管理操作模型、业务连续性管理政策、业务连续性管理目标、业务连续性管理评估和改进，以及管理层在资源管理和人员培训中的职责。	1. 询问了相应人员，以了解阿里云为业务连续性管理而制定的业务连续性管理政策和程序，以及每年审查相关政策和程序的流程。 2. 检查了业务连续性管理文档和《阿里云信息技术管理体系手册》，以确认制定了相关政策和程序用以规范业务连续性管理。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次业务连续性管理政策。	未发现异常情况。
BCR_02	阿里云制定了《阿里云信息服务可用性管理规定》，以确保信息技术服务的可用性和持续有效性满足客户对服务质量的要求。该政策定义了相关方的角色和职责以及可用性管理操作的标准。	1. 询问了相应人员，以了解阿里云用于管理其交付给客户的信息技术服务的可用性和持续有效性的程序，以及每年审查相关政策和程序的流程。 2. 检查了信息服务可用性管理文档，以确认制定了政策和程序以确保交付给客户的信息技术服务的可用性和持续有效性。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次信息服务可用性管理政策和程序。	未发现异常情况。
BCR_03	阿里云制定了《阿里云业务连续性管理规定》，旨在就业务连续性管理提供指导。在此政策下，阿里云制定了业务连续性管理框架，其中包括业务影响分析、风险评估、业务连续性管理报告，以及对《应急响应计划》和《业务连续性计划》的维护、实施、测试和持续改进。	1. 询问了相应人员，以了解阿里云为指导业务连续性管理而制定的业务连续性管理政策和程序，以及每年审查相关政策和程序的流程。 2. 检查了业务连续性管理文档，以确认制定了相关政策和程序以指导业务连续性管理。	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次业务连续性管理政策。	
BCR_04	《业务连续性计划》列出了目标、范围、角色和职责、恢复目标、联系人名单维护、应急响应、恢复计划和事件响应计划相关信息。《业务连续性计划》每年审核一次，并根据需要进行更新。	1. 询问了相应人员，以了解阿里云《业务连续性计划》，以及每年审查《业务连续性计划》的流程。 2. 检查了《业务连续性计划》文档，以确认《业务连续性计划》正式列出了目标、范围、角色和职责、恢复时间目标、联系人名单维护、应急响应计划、恢复计划和事件响应计划相关信息。 3. 检查了每年审查业务连续性的支持性证据，以确认至少每年审查一次业务连续性计划。	未发现异常情况。
BCR_05	阿里云制定了《阿里云信息技术管理体系文档记录管理规定》，旨在规范业务连续性管理的文档记录流程，包括业务连续性管理文档的维护、审批、发布、评估和保留。	1. 询问了相应人员，以了解阿里云按照《阿里云信息技术管理体系文档记录管理规定》管理业务连续性管理的文档的情况，以及每年审查文档管理政策的流程。 2. 检查了《阿里云信息技术管理体系文档记录管理规定》，以确认制定了相关政策和程序用以管理业务连续性管理相关的文档。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次业务连续性文档管理政策。	未发现异常情况。
BCR_06	阿里云制定了《阿里云总体应急预案》，以确定应急响应中的紧急情况分类、角色和职责、工作流程和资源管理。在《阿里云总体应急预案》下，阿里云建立了事件响应程序，旨在详细描述运营和服务、网络和	1. 询问了相应人员，以了解阿里云现有的应急响应计划和事件响应程序用于管理在发生事件时的角色和职责、工作流程、资源管理、上报和通知流程，以及每年审核应	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	IDC 基础设施相关关键事件中的角色和职责、工作流程、恢复时间目标以及上报和通知流程。	急响应计划和事件响应程序的流程。 2. 检查了应急响应计划和事件响应流程，以确认阿里云制定了相关政策和程序，以确立应急响应和事件处理的紧急情况分类、角色和职责、工作流程、资源管理以及上报和通知流程。 3. 检查了每年审查相关政策和程序的支持性证据，以确认至少每年审查一次应急响应计划和事件响应程序。	
BCR_07	阿里云至少每年开展一次对阿里云关键服务和运营业务连续性计划的测试。如测试结果与预期之间存在任何差异，相关负责团队会评估测试结果并且重新开展测试直到测试成功为止。	1. 询问了相应人员，以了解测试阿里云关键服务和运营业务连续性计划的流程。 2. 检查了所选阿里云关键服务和运营业务的连续性测试计划和结果，以确认业务连续性计划的测试至少每年进行一次，测试结果有记录下来并由适当的人员进行审核，并且有跟进测试结果与预期存在差异的情况。	未发现异常情况。
BCR_08	阿里云已建立事件响应程序，以详细说明在发生 IDC 事件时的角色和职责以及工作流。阿里云还制定了应急响应计划来解决 IDC 中断的不同场景，包括火灾、网络中断、紧急断电和自然灾害。	1. 询问了相应人员，以了解阿里云现有的事件响应程序和应急计划用于管理在发生 IDC 事件时的角色和职责以及工作流程，以及每年审核事件响应程序和应急计划所用的流程。 2. 检查了事件响应程序和应急计划，以确认制定了政策和程序，详细说明在发生 IDC 事件时的角色和职责以及工作流程。 3. 检查了每年审查相关政策和程序的支持性证据，以确认至少每年审核一次事件响应程序和应急计划。	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
BCR_09	阿里云每年至少一次在业务中断情况下对数据中心关键流程的持续运营和必要资源的业务连续性进行测试	1. 询问了相应人员，以了解阿里云数据中心业务中断情况下关键流程的持续运营和必要资源的业务连续性测试。 2. 检查了数据中心样本中的业务连续性的测试计划和结果，以确认数据中心业务连续性计划至少每年测试一次，并记录测试结果。	未发现异常情况。
BCR_10	业务连续性管理团队每年执行业务影响分析和风险评估，包括确定关键业务流程、最大可容忍中断时间、恢复时间目标、最低服务水平和恢复服务所需的时间。业务影响分析和风险评估的结果记录在《阿里云业务连续性管理体系业务影响分析、风险评估及策略报告》中。该团队识别和记录可能导致阿里云关键业务运营中断的威胁，并针对不同的中断场景制定相应的策略。	1. 询问了相应人员，以了解进行业务影响分析和风险评估的阿里云业务连续性管理程序。 2. 检查了《阿里云业务连续性管理体系业务影响分析、风险评估及策略报告》，以确认阿里云每年都会执行业务影响分析和风险评估，包括确认关键业务流程、最大可容忍中断时间、恢复时间目标、最低服务水平和恢复服务所需的时间，并确认识别了可能导致阿里云关键业务运营中断的威胁，并针对不同的中断场景制定了相应的策略。	未发现异常情况。
BCR_11	阿里云建立了容量管理基线，并评估了由容量限制带来的资源可用性风险。系统实时监控当前所用容量以预测容量需求。系统在预测用量超过预定义的容量阈值时自动启动资源补给程序。	1. 询问了相应人员，以了解监控当前所用容量、预测容量需求和解决容量需求的流程。 2. 检查了容量监控系统的相关代码，以确认在系统内设置了容量管理基线以及容量分析模型以实时监控和评估各可用区资源可用性风险。 3. 检查了容量监控系统，以确认系统实时监控当前资源周转情况并预测未来容量需	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		求。 4. 检查了系统内的容量监控流程，以确认在预测容量需求超过预定义的容量阈值时自动启动资源补给程序。	
BCR_12	阿里云制定了《阿里云业务连续性安全管理规定》，旨在定义已部署系统的冗余要求。	1. 询问了相应人员，以了解阿里云针对已部署系统的冗余要求而制定的政策。 2. 检查了阿里云业务连续性管理文档，以确认阿里云制定了正式政策以明确系统部署的冗余要求。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次业务连续性管理政策。	未发现异常情况。
BCR_13	阿里云购买外部保险以减轻损失事件导致的财务影响。	1. 询问了相应人员，以了解阿里云以减轻损失事件导致的财务影响风险而购买外部保险的情况。 2. 检查了外部保险文件，以确认阿里云已购买外部保险，以减轻损失事件导致的财务影响。	未发现异常情况。
BCR_14	供应链团队每月进行需求预测，并由相应人员批准相应的容量计划。	1. 询问了相应人员，以了解月度需求预测和容量计划流程。 2. 检查了资源计划平台的月度需求预测和容量计划样本，以确认供应链团队进行了需求预测，相应人员批准了相应的容量计划。	未发现异常情况。
BCR_15	阿里云关键系统组件至少一周进行两次全量备份。	1. 询问了相应人员，以了解阿里云关键系统组件的数据备份流程。	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		2. 检查了备份配置，以确认阿里云关键系统组件完成了配置以确保至少一周进行两次全量备份。 3. 检查了备份日志，以确认基于备份设置完成了阿里云关键系统组件的数据备份。	
BCR_16	阿里云关键系统组件跨多个可用区进行复制。	1. 询问了相应人员，以了解阿里云关键系统组件的数据复制流程。 2. 检查了复制配置，以确认阿里云关键系统组件经过配置，可跨多个可用区进行复制。	未发现异常情况。
BCR_17	阿里云关键系统组件的备份经过加密。	1. 询问了相应人员，以了解阿里云关键系统组件的备份加密程序。 2. 检查了备份配置，以确认阿里云关键系统组件的备份经过加密。	未发现异常情况。
BCR_18	阿里云已制定备份恢复程序。阿里云的关键系统组件按月恢复，并自动进行调节，以检查数据完整性。	1. 询问了相应人员，以了解每月对阿里云关键系统组件执行一次的备份恢复程序和数据完整性检查。 2. 检查了月度备份恢复样本，以确认阿里云关键系统组件按月恢复，并进行数据校正。	未发现异常情况。
BCR_19	阿里云关键系统组件的备份由系统监控。如果出现备份错误或故障，则会自动触发全量备份，直到成功完成备份	1. 询问了相应人员，以了解对阿里云关键系统组件备份的监控流程，包括解决备份失败的纠正措施。 2. 检查了备份监控机制，以确定在备份失败的情况下系统会自动触发阿里云关键系统	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		组件的全量备份，直到成功完成备份。	
BCR_ECS_OSS_20	**适用于 ECS 和 OSS** 阿里云通过分布式存储为 ECS 和 OSS 产品提供数据冗余。数据以多副本形式保存，并自动检查一致性。当任何一份副本不可用时，则使用其他副本自动恢复不可用副本中的数据。	1. 询问了相应人员，以了解多个数据副本和一致性检查机制。 2. 检查了还原后端系统中维护的 OSS 和 ECS 数据的流程，以确认启用多个数据副本和一致性检查机制以在一份副本不可用时，自动使用其他副本恢复不可用副本来还原数据。	未发现异常情况。
BCR_ECS_OSS_RDS_21	**适用于 ECS、OSS 和 RDS** 通过 ECS 的镜像复制功能，可以跨不同区域复制镜像，以便进行远程备份。 通过购买跨区域数据复制服务，可对保存在 OSS 中的数据实现远程备份。 在具有本地 SSD 的高可用性版 RDS 运行 MySQL 8.0 版、在具有本地 SSD 的高可用性版 RDS 运行 MySQL 5.7 版和 MySQL 5.6 版的 RDS 实例，支持跨区域远程灾难恢复备份服务。	1. 询问了相应人员，以了解阿里云通过向 ECS 客户提供镜像复制功能、向 OSS 客户提供跨区域数据复制服务，以及向在具有本地 SSD 的高可用性版 RDS 运行 MySQL 8.0 版、在具有本地 SSD 的高可用性版 RDS 运行 MySQL 5.7 版和 MySQL 5.6 版的 RDS 客户提供远程灾难恢复备份服务，来提供跨区域远程备份服务。 2. 检查了 ECS 镜像的远程备份流程，以确认 ECS 产品具有镜像复制功能，客户能够将一个域的 ECS 镜像复制到其他域作为远程备份。 3. 检查了远程备份流程，以确认 OSS 产品提供跨区域数据复制服务，供客户进行跨区域远程备份。 4. 检查了远程备份流程，以确认 RDS 产品向在具有本地 SSD 的高可用性版 RDS 运行 MySQL 8.0 版、在具有本地 SSD 的高可用性版 RDS 运行 MySQL 5.7 版和 MySQL 5.6 版的 RDS 提供远程灾难恢复备份服务，供客户在不同区域建立灾难恢复备	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		份。	
BCR_CDN_22	**适用于 CDN** 存储在 CDN 网络节点的服务器中的客户数据被切片，以增强服务可用性。	1. 询问了相应人员，以了解 CDN 对客户数据的数据切片机制。 2. 检查了存储在 CDN 网络节点的服务器中的数据状态，以确认存储在 CDN 网络节点的服务器中的数据已进行切片，以增强服务可用性。	未发现异常情况。
BCR_IoT_23	**适用于物联网平台** 阿里云物联网平台提供设备影子功能，以确保设备状态可以在云服务器和设备间及时同步，进而确保服务可用性和数据准确性。	1. 询问了相应人员，以了解阿里云物联网平台的设备影子功能。 2. 观察了物联网平台工程师在阿里云物联网平台上执行了创建设备的测试，然后将设备的参数信息作为影子信息上传到云平台。 3. 观察了物联网平台工程师尝试修改在云端维护的影子信息并检查设备信息的状态，同时确定已经修改云端的设备影子信息。	未发现异常情况。
BCR_IoT_24	**适用于物联网平台** 阿里云物联网平台的各个团队执行业务连续性分析，以评估每种产品和服务可能遇到的潜在风险及其对业务的影响。各业务连续性计划已经设计并定期实施，以确保每种产品和服务的稳定运行。	1. 询问了相应人员，以了解针对阿里云物联网平台执行的业务连续性分析和计划。 2. 检查了业务风险评估记录、业务连续性计划和相关测试结果样本，以确认阿里云物联网平执行了业务风险分析、创建了业务连续性计划并根据计划进行了测试，进而确保物联网相关产品的可用性。	未发现异常情况。
BCR_IoT_25	**适用于物联网平台** 阿里云物联网平台的各团队每月对各产品和服务进行资源用量容量分析，以确认是否需要额外资源。	1. 询问了相应人员，以了解阿里云物联网平台容量分析和使用的情况。 2. 检查了容量分析结果样本，以确认阿里云	未发现异常情况。

控制目标 8: 业务连续性管理			
控制合理保证了在中断后能够及时恢复关键业务			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		物联网平台的相关团队每月对各产品和服务进行了资源容量计划，以分配资源。	
BCR_IoT_26	适用于物联网平台 阿里云物联网平台采用具有高可用性配置的数据库进行数据存储。各产品和服务的主从数据库实例在不同的可用区进行维护，以实现异地备份。	1. 询问了相应人员，以了解阿里云物联网平台数据存储的高可用性配置。 2. 检查了数据库配置样本，以确认产品相关数据被复制到两个不同的物理数据中心，以实现异地备份。	未发现异常情况。
DCS_10	阿里云为数据中心部署了网络设备的双路供电和双机热备。不间断电源（UPS）和内部柴油发电机已安装在数据中心，以便在出现电气故障时提供备用支持。	1. 询问了相应人员，以了解在数据中心部署的网络设备的双路供电和双机热备的情况。 2. 检查了数据中心的电源设备、电路图、网络设备监控系统和网络拓扑结构，以确认为数据中心部署了网络设备的双路供电和双机热备，并在数据中心安装了不间断电源 (UPS) 和内部柴油发电机。	未发现异常情况。
IPY_02	阿里云在阿里云网站上发布了开放 API，以支持与云服务的交互以及组件之间的互操作性。	1. 询问了相应人员，以了解阿里云提供的开放 API 的情况。 2. 检查了阿里云开放平台上发布的 API，以确认在该开放平台上发布了适用于多类阿里云服务的开放 API。	未发现异常情况。

控制目标 9: 事件管理			
控制合理保证了可以及时识别、分析、处理和记录来自每个系统模块的事故和事件。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
SEF_01	阿里云制定了《安全事件、漏洞应急处理体系》，以规范事件的管理、分类及响应机制，且包括对不同级别事件响应时间的要求以及相应的	1. 询问了相应人员，以了解根据《安全事件、漏洞应急处理体系》的规定对安全事件进行分类并采用相应的响应机制的情况，以及每年审查安全事件管理	未发现异常情况。

控制目标 9: 事件管理			
控制合理保证了可以及时识别、分析、处理和记录来自每个系统模块的事故和事件。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	解决方案。	政策的流程。 2. 检查了安全事件响应程序文档，以证实严格执行了相关政策，以确保所有信息服务相关的安全事件均按照一致的标准进行分类并相应响应。 3. 检查了每年审查相关政策的支持性证据，以证实至少每年审查一次安全事件管理政策。	
SEF_02	阿里云使用安全事件监控平台来分析生产系统内执行的活动的日志，并根据既定的审核规则识别异常用户操作和安全事件。安全事件由安全团队审查和监控以确保事件得到处理。	1. 询问了相应人员，以了解安全事件监控流程及相应的平台。 2. 检查了安全事件监控平台，以确认系统根据既定的审核规则监控异常用户操作和安全事件。 3. 检查了已识别安全事件的样本，以确认事件审查和处理是否由安全团队执行和监控。	未发现异常情况。
SEF_03	数据中心发生事件后，数据中心服务提供商将根据事件的风险等级和性质向阿里云提交操作事件报告，其中包含引起事件的原因、影响和解决状态。	1. 询问了相应人员，了解了阿里云已建立的数据中心服务提供商应遵循的事件报告程序，以确保数据中心服务提供商会对数据中心发生的事件进行适当的记录、分析和解决，并及时与阿里云沟通。 2. 检查了数据中心服务提供商提供给阿里云的操作事件报告样本，以确认数据中心服务提供商对事件进行了记录、分析和跟踪，直至解决。	未发现异常情况。
SEF_04	阿里云制定了《故障管理标准》，以规范安全故障的分类、上报、通知和解决流程。	1. 询问了相应人员，以了解根据《故障管理标准》规范故障分类标准、制定及时解决故障要求及根据风险等级设置建立相应解决方案的情况，以及每年审查故障管理政策的流程。 2. 检查了故障管理文档，以确认严格执行了相关政策，以确保所有信息服务的故障均按照一致的标准	未发现异常情况。

控制目标 9: 事件管理			
控制合理保证了可以及时识别、分析、处理和记录来自每个系统模块的事故和事件。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		进行分类并相应响应。 3. 检查了每年审查相关政策的支持性证据，以确认至少每年审查一次故障管理政策。	
SEF_05	阿里云利用故障管理平台来整合和跟踪通过不同渠道发现的故障。全球运维中心负责跟踪故障，直到故障得到解决，并与相应团队合作进行进一步的改进。	1. 询问了相应人员，以了解阿里云故障管理平台对已识别的故障进行汇总和评估，并支持相应的处理程序和纠正措施的情况。 2. 检查了故障工单样本和故障管理平台的日志记录，以确认全球运维中心在故障管理平台中记录了故障分类、后续行动、解决状态和强化措施的相关信息。	未发现异常情况。
SEF_06	安全团队每月组织一次内部会议，对过去一个月发生的故障进行根因分析，并与业务领导层和项目经理讨论解决状态。	1. 询问了相应人员，以了解安全团队如何召开月度安全事件和故障分析会议，以及如何分析事件模式和制定后续解决行动。 2. 检查了月度会议记录样本，以确认安全团队每月组织一次内部会议，对过去一个月发生的故障进行根因分析，并与业务领导层和项目经理讨论解决状态。	未发现异常情况。
SEF_07	阿里云建立了多通道沟通机制，包括阿里云官方网站、站内信、短信、电子邮件和钉钉消息，用于通知可能影响客户的故障。	1. 询问了相应人员，以了解用于通知可能影响客户的故障的多通道沟通机制。 2. 检查了可能影响客户的故障的样本，以了解向客户发送的故障管理平台内的故障信息及相应的故障通知，以确认阿里云会通过官方网站或站内信、短信、电子邮件和钉钉消息向客户通知对其有影响的故障。	未发现异常情况。
SEF_CDN_08	**适用于 CDN** 如果发生本地节点故障，CDN 会根据预设规则将故障节点的内容切换到正常运作的邻近节点。	1. 询问了相应人员，以了解 CDN 将故障节点的内容自动切换到邻近节点的机制，以确保服务连续性。	未发现异常情况。

控制目标 9: 事件管理			
控制合理保证了可以及时识别、分析、处理和记录来自每个系统模块的事故和事件。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
		2. 观察了软件工程师执行使 CDN 节点出现故障以中断正常操作的测试，以确认 CDN 自动讲故障节点的连接请求切换至另一邻近节点。	
TVM_05	阿里云制定了《安全事件、漏洞应急处理体系》，以规范安全漏洞管理，包括安全漏洞的分类和响应机制。	1. 询问了相应人员，以了解根据《阿里云安全事件、漏洞应急处理体系》规范安全漏洞评估和分类流程的情况，以及每年审查安全事件管理政策的流程。 2. 检查了《安全事件、漏洞应急处理体系》，以确认阿里云制定了安全漏洞管理相关的正式政策（包括定期的漏洞识别与分析，后续的防御措施，是否通知了客户或是否要求相关人员进行了确认）以解决已识别的漏洞，以及确认了至少每年审查一次该标准。	未发现异常情况。
TVM_06	安全团队编制安全事件和安全漏洞的汇总表，并每月向管理层报告。	1. 询问了相应人员，以了解在月度安全运行会议上向管理层报告安全事件和安全漏洞的情况。 2. 检查了月度安全运行会议记录的样本，以确认安全团队每月向最高管理层报告安全漏洞，且之前是别的安全漏洞均已被解决。	未发现异常情况。
TVM_07	阿里云使用漏洞扫描系统对云环境中的安全漏洞执行至少每日一次的全方位扫描。扫描结果会自动提交到安全漏洞管理平台。	1. 向相应人员询问。以了解漏洞扫描程序，以及确认用于开发和提供云服务的所有 IT 系统是否都是漏洞扫描流程的一部分。 2. 检查了漏洞扫描系统的配置设定，以确定漏洞扫描系统用于对云环境中的安全漏洞执行至少每日一次的全方位扫描。 3. 检查了漏洞扫描系统的扫描结果样本，以确认被确认为漏洞的安全事件已被自动录入到安全漏洞管理平台。	未发现异常情况。
TVM_08	阿里云通过多种渠道（包括内部报告、外部报	1. 询问了相应人员，以了解安全事件和漏洞的管理和	未发现异常情况。

控制目标 9: 事件管理			
控制合理保证了可以及时识别、分析、处理和记录来自每个系统模块的事故和事件。			
控制 ID	**阿里云的控制描述**	**PwC 的测试程序**	**PwC 的测试结果**
	告、从外部漏洞发布平台订阅以及通过扫描进行内部检测）收集和检测安全事件和漏洞。安全事件和漏洞汇总至安全事件和漏洞管理平台。安全团队每天审查事件和漏洞，并任命恰当的人员对其进行处理。	记录程序。 2. 检查了安全事件和漏洞管理平台的接口，以确认阿里云使用安全事件和漏洞管理平台来收集内外部报告的安全漏洞。 3. 检查了阿里云网站上的客户安全通知，以确认阿里云会向客户告知安全风险和漏洞并提供相关建议。 4. 检查了安全漏洞解决日志的样本，以确认日志被用于支持和记录安全漏洞的分类、任务分配及恢复和检查过程。	
TVM_09	外部第三方每半年进行一次渗透测试。记录并分析所识别出的漏洞，必要时采取纠正措施。	1. 询问了相应人员，以了解外部渗透测试程序。 2. 检查了外部渗透测试文档，以确认半年度报告中包含所发现的漏洞，其各自的风险等级和描述，以及所定义的对云服务的安全运行至关重要的基础架构组件。 3. 检查了所发现的中/高重要性等级漏洞的跟进文档，以确认跟进并修复了所发现的对云服务的保密性、安全性或可用性有重大影响的漏洞。	未发现异常情况。

第五节——服务审计师报告中未涵盖的阿里云提供的其他信息

阿里云信息安全与合规

云安全和用户隐私是阿里云在向客户提供服务时的最高优先事项。为确认其实践符合行业最佳实践以及相关信息安全和隐私要求，阿里云聘请了独立第三方定期验证现有控制并获得了相关资质。阿里云还参与制定了多项云行业标准，并为最佳实践标准的制定做出了贡献。阿里云的安全性和合规性得到全球权威认可。

作为中国大陆最大的云服务提供商，阿里云计算有限公司于 2013 年 6 月获得中华人民共和国工业和信息化部（“工信部”）签发的跨区域增值电信服务（网络数据中心和网络访问）业务经营许可证。根据中国国家增值电信服务管理要求，阿里云计算有限公司在中国使用的数据中心已通过工信部审核和验证；同时，阿里云计算有限公司接受工信部每年针对增值电信服务提供商的资源管理系统、信息安全系统、档案系统和网络安全系统的检查。此外，阿里云还于 2019 年通过了等级保护 2.0 (等保 2.0) 3 级，是首批通过该标准的公共云服务提供商之一。

此外，阿里云也已经过验证，符合以下领先实践的标准和要求：

- ISO/IEC 20000:2011 信息技术服务管理体系
- ISO/IEC 22301:2012 业务连续性管理体系
- ISO/IEC 27001:2013 信息安全管理体系
- ISO/IEC 27017:2015 基于 ISO/IEC 27002 的云服务信息安全控制实践守则
- ISO 9001:2015 质量管理体系
- ISO/IEC 27018:2019 作为 PII 处理者在公共云中保护个人身份信息 (PII) 的实践守则
- 隐私信息管理 ISO/IEC 27701:2019 扩展至 ISO/IEC 27001 和 ISO/IEC27002
- BS 10012 个人信息管理
- 云安全联盟安全、信任、保障和风险（“CSA STAR”）认证
- 支付卡行业数据安全标准（“PCI DSS”）认证
- 支付卡行业三个域安全（“PCI 3DS”）核心安全标准认证
- TRUSTe 企业隐私认证
- 亚太经合组织跨境隐私规则体系认证
- 亚太经合组织数据处理者隐私识别体系认证
- 新加坡——多层云计算安全（“MTCS”）T3 认证
- 新加坡——个人数据保护行为（“PDPA”）合规评估
- 新加坡——数据保护信任标识 (DPTM) 认证
- 阿联酋——国家电子安全局（“NESA”）签发的标准和指南 P1 级合规
- 阿联酋——迪拜政府信息安全规范（“ISR”）
- 美国——健康保险携带和责任法案（“HIPAA”）要求
- 美国——美国电影协会（“MPAA”）最佳实践指南
- 美国——GxP 准备评估
- 美国——可信合作伙伴网络认证
- 德国——云计算合规控制目录 (C5)
- 德国——可信云认证
- 德国——可信信息安全评估交换（“TiSAX”）
- 中国——可信云服务认证
- 中国——云产品合格评定国家认可委员会（“CNAS”）
- 中国——公安部签发的安全服务能力认证
- 中国——中国电子工业标准化技术协会 ITSS 分会（由工信部指导）的云服务能力认证（高级）
- 中国——等级保护 2.0（等保 2.0）金融云 4 级，公共云 3 级

回应新冠肺炎（ COVID-19 ）对阿里云服务的影响

为应对 2020 年 1 月爆发的新冠肺炎疫情 （COVID-19），阿里云建立了应急响应机制，以指导远程工作和运营。疫情期间，为避免由于远程办公和隔离而可能增加的网络攻击，阿里云并未放松对相关控制的执行。相反，阿里云在疫情期间的控制成果验证了阿里云应急计划的有效性以及快速应急响应的能力。另外，阿里云基于自身的控制和安全能力，为用户机构提供云安全特性和安全服务帮助他们实现被疫情加速的数字化转型。综上，疫情对阿里云的控制有效性和服务并未产生实质性影响。