华为云 ISO/IEC 27001 合规性说明

文档版本 1.0

发布日期 2021-07-16

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 概述

1.1 适用范围

本文档提供的信息适用于华为云在中国站上开放的产品和服务，以及承载这些产品和服务的数据中心节点。

1.2 发布目的与目标读者

国际标准化组织（ISO）发布的ISO/IEC 27001:2013是目前在国际上被广泛接受和应用的信息安全管理体系（ISMS）认证标准，该标准可用于帮助组织设计和建立信息安全管理体系。ISO 27001以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体系的持续运行。

华为云参照ISO/IEC 27001:2013构建了完善的信息安全管理体系，同时制定了华为云整体的信息安全策略，并获得ISO/IEC 27001:2013信息安全管理体系认证。

本文档将通过对ISO/IEC 27001:2013的正文部分及附录A中14个控制域进行应答，向客户展示华为云的整体信息安全策略及具体控制措施，帮助其了解：

- ISO/IEC 27001:2013中各控制域主要的控制要求以及华为云如何符合其要求；
- 华为云为客户提供了多种产品帮助其建立信息安全管理体系并实现ISO/IEC 27001:2013标准中的控制目标。

1.3 基本定义

- **华为云**：华为云是华为的云服务品牌，致力于提供稳定可靠、安全可信、可持续创新的云服务。
- **客户（租户）**：指与华为云达成商业关系的注册用户，在本文中同租户含义一致，即使用华为云云服务的用户组织，在本文部分场景中使用租户这一表述。
- **国际标准化组织（ISO）**：ISO是一个独立的非政府国际组织，拥有165个国家标准机构成员。通过其成员，它汇集了专家来分享知识，并制定自愿的、基于共识的且与市场相关的国际标准，以支持创新并为全球挑战提供解决方案。

2 ISO 27001 简介

2.1 ISO 27001 的框架和主要内容

ISO/IEC 27001:2013是目前国际上最为通行的信息安全管理体系指导标准和最佳实践。它提出了在组织范围内建立、实施、维护和持续改进信息安全管理体系的要求以及根据组织的需要评估和处理信息安全风险的要求。

《ISO/IEC 27001:2013信息技术-安全技术-信息安全管理体系-要求》分为正文和附录A两个主要部分。第一部分对信息安全管理给出建议，供负责在其组织启动、实施或维护安全的人员使用；第二部分说明了建立、实施和文件化信息安全管理体系（ISMS）的要求，规定了根据独立组织的需要应实施安全控制的要求。

控制被总结成14个安全域，当组织正确实施安全控制时，可以通过解决在正式的、定期的风险评估中确定的特定问题，帮助组织实现和保持信息安全合规性。

ISO/IEC 27001:2013中的14个安全域及内容简介如下：

- A.5 信息安全策略：依据业务要求和相关法律法规为信息安全提供管理指导和支持。
- A.6 信息安全组织：建立一个管理框架，开展组织的信息安全工作。
- A.7 人力资源安全：确保员工和外包方理解并履行其信息安全职责，在任用终止时保护公司的利益。
- A.8 资产管理：识别组织信息资产，按照信息资产的重要程度确定适当的防护级别。确保存储在介质中的信息资产不会遭到泄露或破坏。
- A.9 访问控制：限制对信息和信息处理设施的访问，保证授权用户对系统和服务的访问，并阻止未授权的访问。
- A.10 密码：有效使用密码技术以保护信息的保密性、真实性、完整性。
- A.11 物理和环境安全：阻止对信息和信息处理设施的未授权物理访问、损坏和干扰。防止资产的丢失、损坏、失窃或危及资产安全、业务连续性。
- A.12 运行安全：确保正确、安全地操作信息处理设施并采用技术手段防范恶意代码。使用备份以防止数据丢失，采用日志和监视手段，记录事态并生成证据。确保运行系统的完整性，防止对技术脆弱性的利用，使审计活动对系统运行的影响最小化。
- A.13 通信安全：网络及其支持性信息处理设施中的信息应得到保护。保证在公司内、外传输信息的安全。

- A.14 系统获取、开发和维护：信息安全是信息系统生命周期中的一个有机组成部分，信息安全在信息系统开发生命周期中应有相应的设计和实施。用于测试的数据应得到保护。
- A.15 供应商关系：确保供应商可访问的信息资产受到保护。保持与供应商协议一致的信息安全服务交付。
- A.16 信息安全事件管理：采用有效的方法对信息安全事件进行管理，包括对安全事件和风险的沟通。
- A.17 业务连续性管理的信息安全方面：将信息安全连续性纳入公司业务连续性管理之中。使信息处理设施具有足够的冗余以满足可用性要求。
- A.18 符合性：避免违反与信息安全有关的法律、法规、规章和合同义务以及任何安全要求。开展信息安全评审，确保依据组织方针策略、规程开展信息安全工作。

2.2 标准适用群体

ISO/IEC 27001:2013中规定的要求是通用的，旨在适用于所有组织，无论类型、规模或性质。

3 华为云的认证情况

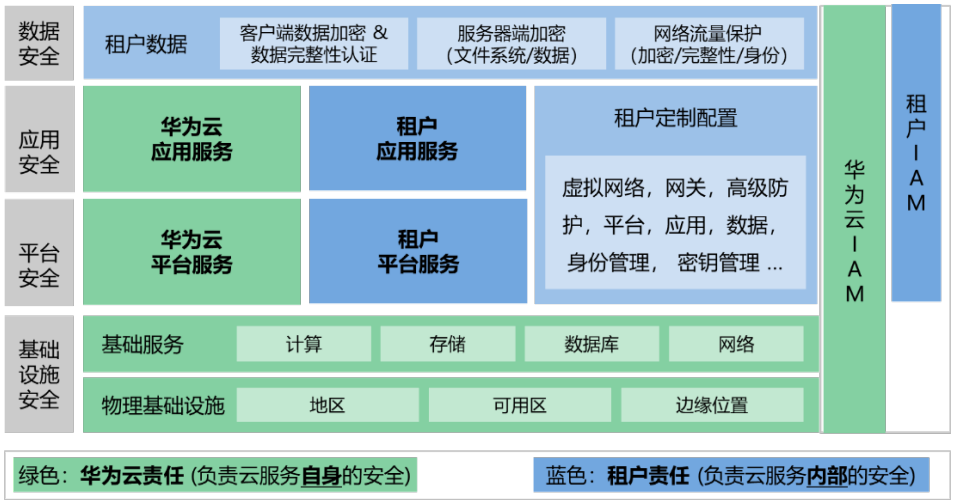
华为云凭借自身的信息安全管理体系及安全控制措施管理获得了ISO/IEC 27001:2013认证，认证范围涵括华为云在其官网发布的产品及服务，以及遍布全球多地的数据中心。

如需了解ISO/IEC 27001:2013的认证范围及认证活动详情，可在华为云**信任中心-合规**下载ISO/IEC 27001:2013证书作为参考。

4 华为云责任共担模型

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要客户与华为云共同努力。基于此，华为云为帮助客户理解双方的安全责任边界、避免出现安全责任真空区而提出了责任共担模型。在模型中客户与华为云具体负责的区域可参见下图。

图 4-1 责任共担模型



基于责任共担模型，华为云与客户主要承担如下责任：

华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和用户身份管理（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

客户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对用户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，用户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

关于华为云与用户的安全责任详情，可参考华为云已发布的《华为云安全白皮书》。

5 华为云如何遵循 ISO 27001 标准要求

本文档使用的ISO 27001标准要求中的控制措施参考2016年发布的国家标准《 GB/T 22080-2016/ISO/IEC 27001：2013 信息技术 安全技术 信息安全管理体系 要求 》。

5.1 ISO 27001 标准正文部分

华为云根据ISO 27001的要求建立并实施信息安全管理体系，并在日常运营中遵循PDCA循环模型对其进行维护和持续改进，在体系建立初期确定内外部环境并识别相关方需求，以确定信息安全管理体系的范围。在组织方面，华为云通过自上而下的治理结构实现信息安全，由领导层决策和审批信息安全策略和目标、信息安全相关角色和职责，制定相应的信息安全计划、分配执行信息安全活动所需的资源，同时为体系内其他角色提供支持，促进体系持续改进。为促进与外部的顺畅沟通，华为云配备专人与行政机构、风险和合规组织、地方当局和监管机构保持联系并建立联络点。

依据ISO 27001信息安全管理体系要求，华为云建立了信息系统相关文档，包括文档化的信息安全政策和程序，为华为云的操作和信息安全管理提供指导。员工可根据授权查看已发布的信息安全政策和程序。华为云至少每年审查一次信息安全管理体系文档，并根据需要予以更新，以反映业务目标或风险环境的变更情况。信息安全政策和程序的变更需要获得高级管理层的审批。

华为云制定了信息安全风险评估方法，从多个维度识别风险，并根据安全策略、安全技术、安全稽核的完备程度对风险的可能性进行判断，同时根据要求定期执行信息安全风险评估。风险评估涵盖信息安全的各方面，包括数据保护和分类、数据留存和传输位置、数据保存时间对法律法规的符合等。风险评估的目的是识别华为云的威胁和漏洞，基于业务流程和资产管理情况，为威胁和漏洞分配风险评级，对评估进行正式记录并制定风险处置计划。风险评估报告完成后由高级管理层进行审批。

华为云建立了自己的培训机制，根据不同的角色、岗位为员工设计合适的培训方案。新员工转正前必须通过有关网络安全与隐私保护的上岗培训和考试；在岗员工需根据不同业务角色，选择相应课程进行学习与考试，其中一般员工的培训频率为至少每年一次，核心岗位员工培训频率更高。管理者需参加网络安全培训和研讨。针对安全意识，华为云对全员进行相关培训，以帮助员工了解组织信息安全方针及政策等，同时员工须承诺遵守公司各项安全政策和制度要求。

华为云建立了正式的、定期的审计计划，包括持续的、独立的内部和外部评估，内部评估持续追踪安全控制措施的有效性，外部评估以独立审核员身份进行审计，以验证华为云控制环境的实施和运行有效性。同时华为云每年定期开展管理评审，识别体系运行过程中的问题并实施整改，推动管理体系的持续改进。

5.2 ISO 27001 标准附录 A（规范性附录）参考控制目标和控制措施

- **A.5 信息安全策略**

信息安全管理指导策略的目标是依据业务要求和相关法律法规，为信息安全提供指导和支持。

编号	控制域	控制措施	华为云的回应
A.5.1.1	信息安全策略	信息安全策略集应被定义，由管理者批准，并发布、传达给所有员工和外部相关方。	华为云实施文档化的信息安全政策和程序，为操作和信息安全管理提供指导。信息安全政策和程序发布前需得到管理者审批，员工可根据授权查看已发布的信息安全政策和程序。
A.5.1.2	信息安全策略的评审	应按计划的时间间隔或当重大变化发生时进行信息安全策略评审，以确保其持续的适宜性、充分性和有效性。	华为云至少每年审查一次信息安全管理策略和流程，并根据需要予以更新，以反映业务目标或风险环境的变更情况。政策及流程的变更需要获得高级管理层的审批。

- **A.6 信息安全组织**

信息安全组织目标包括内部组织目标，即建立一个管理框架以启动和控制组织内信息安全的实现和运行。以及确保组织内人员远程工作和使用移动设备时的安全。

编号	控制域	控制措施	华为云的回应
A.6.1.1	信息安全角色和责任	所有的信息安全职责宜予以定义和分配。	华为云在各产品、服务的业务团队中明确规定了所有员工对应角色的信息安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的信息安全管理职责。信息安全相关的角色和职责通过书面的方式确定并获得高级领导层的审批。
A.6.1.2	职责分离	应分离冲突的职责及其责任范围，以减少未授权或无意的修改或者不当使用组织资产的机会。	华为云遵循职责分离和权限制衡原则，对不相容职责进行分离，实现合理的权限分工，同时制定了SOD权责分离管理矩阵以帮助实现该管理原则。

A.6.1.3	与职能机构的联系	应维护与相关职能机构的适当联系。	华为云配备了专人与行业机构、风险和合规组织、地方当局和监管机构保持联系并建立联络点。
A.6.1.4	与特定相关方的联系	应维护与特定相关方、其他专业安全论坛和专业协会的适当联系。	同A.6.1.3
A.6.1.5	项目管理中的信息安全	应关注项目管理中的信息安全问题，无论何种类型的项目。	华为云在项目管理中将安全目标纳入项目目标，在项目初期对其进行信息安全风险评估并在整个项目交付过程中定期评审信息安全影响。
A.6.2.1	移动设备策略	应采用相应的策略及其支持性的安全措施以管理由于使用移动设备所带来的风险。	华为云制定了移动设备管理规定，以实施对移动计算设备的统一管理。对移动设备使用的原则、职责、权限要求、设备管理安全要求、网络接入要求及违规处罚等均做出规定并实施。针对便携电脑，机要岗位不配备便携电脑，当便携电脑进入受控区域时需获得批准，同时对便携电脑采取措施以防止丢失后发生数据泄露。
A.6.2.2	远程工作	应实现相应的策略及其支持性的安全措施，以保护在远程工作地点上所访问的、处理的或存储的信息。	华为云员工在内部办公网络中使用唯一身份标识。当需要从外部网络接入华为内部办公网络时，需通过VPN接入。 针对运维场景，华为云通过在数据中心部署的VPN和堡垒机实现运维管理平台的统一运维管理和审计。数据中心外网运维人员和内网运维人员对网络、服务器等设备的本地及远程操作全部集中管理，实现用户对设备资源操作管理的统一接入、统一认证、统一授权、统一审计。 为实现对华为云的远程管理，不论是从互联网还是办公网接入，都要首先访问资源池堡垒机，再从堡垒机访问相关资源。

- **A.7 人力资源安全**

人力资源安全目标包括任用前确保员工和合同方理解其责任、并适合其角色，任用中确保员工和合同方意识到并履行其信息安全责任，以及在任用变更或终止时保护组织的利益。

编号	控制域	控制措施	华为云的回应
A.7.1.1	审查	应按照相关法律法规和道德规范，对所有任用候选者的背景进行验证核查，并与业务要求、访问信息的等级和察觉的风险相适宜。	在适用法律允许的情况下，华为云会根据可接触的资产的机密性，在聘用员工或外部人员前对其进行背景调查。同时为了内部有序管理，消减人员管理风险对业务连续性和安全性带来的潜在影响，华为云对运维工程师等重点岗位实施专项管理，包括上岗安全审查、在岗安全培训赋能、上岗资格管理、离岗安全审查。
A.7.1.2	任用条款及条件	应在员工和合同方的合同协议中声明他们和组织对信息安全的责任。	员工与公司签署的聘用协议中包含保密条款，其中明确说明员工的信息安全责任。对于合同方，华为云与其签署保密协议并进行信息安全培训，其中包含信息安全责任。
A.7.2.1	管理责任	管理者应要求所有员工和合同方按照组织已建立的策略和规程应用信息安全。	华为云已制定针对公司各类人员的信息安全管理要求，对华为员工、机要岗位员工及外部人员提出分层分级的信息安全管理要求。 针对员工，在其与公司签署的聘用协议中包含保密条款，并明确员工的信息安全责任。 针对外部人员，华为云接口部门在与之签署的合同或协议条款中明确约定对外部人员及所属公司的信息安全管理要求，以及信息安全违规处罚措施。
A.7.2.2	信息安全意识、教育和培训	组织所有员工和相关的合同方，应按其工作职能，接受适当的意识教育和培训，及组织策略及规程的定期更新的信息。	在培养员工安全意识方面，华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的形式包括但不限于现场演讲、视频网课等。

A.7.2.3	违规处理过程	应有正式的、且已被传达的违规处理过程以对信息安全违规的员工采取措施。	华为建立了严密的安全责任体系，贯彻违规问责机制。华为云以行为和结果为主要依据对员工进行问责。根据华为云员工安全违规的性质，以及造成的后果确定问责处理等级，分级处理。对触犯法律法规的，移送司法机关处理。直接管理者和间接管理者存在管理不力或知情不作为的，须承担管理责任。违规事件处理根据违规个人态度与调查配合情况予以加重或减轻处理。 华为云的违规政策供所有员工进行查看学习，并定期组织培训提升员工对违规行为、违规后果、惩罚措施的了解。
A.7.3.1	任用终止或变更的责任	应确定任用终止或变更后仍有效的信息安全责任及其职责，传达至员工或合同方并执行。	华为云规定员工离职时需签署离职保密承诺书，确认其应持续承担的信息安全责任及职责。 对于外部人员，华为云接口部门根据业务需要与其所属组织签署保密协议。

- **A.8 资产管理**

资产管理的目标为首先识别组织资产并定义适当的保护责任，确保信息按照其对组织的重要程度受到适当水平的保护，以及防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。

编号	控制域	控制措施	华为云的回应
A.8.1.1	资产清单	应识别信息，以及信息和信息处理设施相关的其他资产，并编制和维护这些资产的清单。	根据ISO 27001标准，华为云对信息资产进行分类并由专门的工具进行监控和管理，形成资产清单，每个资产均被指定所有者。
A.8.1.2	资产的所属关系	应维护资产清单中资产的所属关系。	同A.8.1.1
A.8.1.3	资产的可接受使用	应识别可接受的信息使用规则，以及与信息和信息处理设施有关的资产的可接受的使用规则，形成文件并加以实施。	华为云已制定并实施资产的使用规则，包括管理原则、相关人员职责、办公计算机安全要求、办公网络安全要求、办公应用系统安全要求、存储介质与端口安全要求、办公外设安全要求、非华为计算机安全要求以及相关违规的处罚等。

A.8.1.4	资产归还	所有员工和外部用户在任用、合同或协议终止时，应归还其占用的所有组织资产。	华为云制定了人员安全相关管理规定，要求员工离职或离岗时向公司移交所持有的华为云资产。与合作伙伴合同/业务关系终止时，按照合作协议删除自带设备中在合作项目中产生的信息，并移交华为云提供的资产。华为云建立了人员离职/合作终止时的资产交接电子流，按照电子流程执行资产交接。
A.8.2.1	信息的分级	信息应按照法律要求、价值、重要性及其对未授权泄露或修改的敏感性进行分级。	华为云对数据进行分级管理，结合机密性、完整性、可用性、合规性进行综合定级，将数据分为多个安全级别并分别给出该级别数据的定义。同时规定了不同级别数据的安全实施要求、稽查要求以及应急响应及演练要求。各业务领域遵照数据定级标准对其领域内数据标记安全等级。
A.8.2.2	信息的标记	应按照组织采用的信息分级方案，制定并实现一组适当的信息标记规程。	同A.8.2.1
A.8.2.3	资产的处理	应按照组织采用的信息分级方案，制定并实现资产处理规程。	同A.8.2.1
A.8.3.1	移动介质的管理	应按照组织采用的分级方案，实现移动介质管理规程。	华为云制定并实施移动介质管理规定，各类移动介质由专人管理，借用时需要审批，使用完毕后须进行格式化处理。对个人存储介质及数字设备进出不同安全保密级别的区域及其使用均制定了不同的安全要求。
A.8.3.2	介质的处置	应使用正式的规程安全地处置不再需要的介质。	华为云制定并实施介质管理规定，其中对介质清退报废进行分类操作，通过多种方式实现数据清除、磁盘消磁，并对销毁操作进行记录。
A.8.3.3	物理介质的转移	包含信息的介质在运送中应受到保护，以防止未授权访问、不当使用或毁坏。	同A.8.3.1

- **A.9 访问控制**

访问控制的业务要求目标为限制对信息和信息处理设施的访问。针对用户，应确保授权用户对系统和服务的访问，并防止未授权的访问，并让用户承担保护其鉴别信息的责任。针对系统和应用，应防止对系统和应用的未授权访问。

编号	控制域	控制措施	华为云的回应
A.9.1.1	访问控制策略	应基于业务和信息安全要求，建立访问控制策略，形成文件并进行评审。	华为云员工账号管理遵从公司用户账号权限管理规定。针对华为云云平台账号，华为云制定了公有云账号权限管理要求及流程。对账号进行分类管理并建立访问控制策略，相关文件均通过评审流程并发布。
A.9.1.2	网络和网络服务的访问	应仅向用户提供他们已获专门授权使用的网络和网络服务的访问。	华为云根据不同业务维度和相同业务不同职责，实行RBAC权限管理。登录权限分为：核心网络、接入网络、安全设备、业务系统、数据库系统、硬件维护、监控维护等。不同岗位不同职责人员限定只能访问本角色所管辖的设备，其他设备无权访问。
A.9.2.1	用户注册和注销	应实现正式的用户注册及注销过程，以便可分配访问权。	华为云员工在内部办公网络中使用唯一身份标识，已建立完善的账号生命周期管理规定及流程。 对云服务的访问通过**统一身份认证服务（IAM – Identity and Access Management）**对用户进行访问控制和权限管理。 所有运维账号，设备及应用的账号均进行统一管理，以确保实现从创建用户、授权、鉴权到权限回收的全流程管理。如果账号使用人要使用账号，账号管理员可启动授权流程，通过口令或者提升账号的权限等方式进行授权；账号的申请人和审批人不能是同一个人。
A.9.2.2	用户访问供给	应对所有系统和服务的所有类型用户，实现一个正式的用户访问供给过程以分配或撤销访问权。	同A.9.2.1

A.9.2.3	特许访问权管理	应限制并控制特许访问权的分配和使用。	华为云针对特权账号制定了管理要求，将特权账号分类并在特权账号创建、回收、授权、使用、注销等各阶段中遵守管理要求。 华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，特权账号被严格纳管回收，员工每次登陆均需要使用多重身份验证确定身份。
A.9.2.4	用户的秘密鉴别信息管理	应通过正式的管理过程控制秘密鉴别信息的分配。	华为云制定了密码策略及账号口令安全相关管理规范，对秘密鉴别信息的分配进行管理。新建系统中的账号缺省密码在首次使用前由用户进行更改，当用户需要重置密码时对其身份进行验证。
A.9.2.5	用户访问权的评审	资产拥有者应定期对用户的访问权进行评审。	华为云已规定对不同级别账号/权限的最长审视周期，账号/权限责任人会定期审视其持有的账号/权限，在使用人转岗或角色变化时由责任人提交注销申请。 针对专用账号，账号/权限责任人会审视其负责的专用账号，当不再需要专用账号时修改口令并知会新使用人。 针对外包合作人员账号/权限，管理负责人在外包合作人员离场或不再需要账号/权限时提交注销申请。 主管会审视下属的账号/权限持有情况是否合理，如下属岗位/角色变动，将审视其原有岗位账号/权限是否已注销。
A.9.2.6	访问权的移除或调整	所有员工和外部用户对信息和信息处理设施的访问权在任用、合同或协议终止时，应予以移除，或在变化时予以调整。	同A.9.2.5
A.9.3.1	秘密鉴别信息的使用	应要求用户遵循组织在使用秘密鉴别信息时的惯例。	同A.9.2.4

A.9.4.1	信息访问限制	应按照访问控制策略限制对信息和应用系统功能的访问。	华为云对于内部人员实行基于角色的访问控制及权限管理，限定不同岗位不同职责的人员只能对所授权的目标进行特定操作。通过最小化的权限分配和严格的行为审计，确保人员不会在非授权情况下进行访问。
A.9.4.2	安全登录规程	当访问控制策略要求时，应通过安全登录规程控制对系统和应用的访问。	华为云强调员工云服务账号的安全风险可控，严格要求安全强口令，定期审视账号权限范围，严格纳管回收特权账号。使用IAM对访问进行管理，支持多因素认证用于登录验证和操作保护，员工每次登陆均需要使用多重身份验证确定身份。也提供会话超时策略、账号登陆和锁定策略。
A.9.4.3	口令管理系统	口令管理系统应是交互式的，并应确保优质的口令。	华为云已制定并实施密码策略，包括规定密码长度、复杂度、更改周期，密码中不允许包含用户ID，不可使用易被破解的常用口令以及最近5次使用过的密码等。
A.9.4.4	特权实用程序的使用	对于可能超越系统和应用控制的实用程序的使用应予以限制并严格控制。	华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段。华为云运维人员登入运维管理区时必须先通过**虚拟专用网络（VPN – Virtual Private Network）**接入，再通过堡垒机访问被管理节点。管理员可从此区域访问所有区域的运维接口，此区域不向其他区域开放接口。
A.9.4.5	程序源代码的访问控制	应限制对程序源代码的访问。	华为云信息安全环境采用分区管理。不允许下载源代码，不能从公司外部访问源代码，或通过基础办公应用传输源代码。源代码从公司信息安全环境传出到公司外部须审批受控。

- **A.10 密码**

密码控制目标为确保适当和有效地使用密码技术以保护信息的保密性、真实性和（或）完整性。

编号	控制域	控制措施	华为云的回应

A.10.1.1	密码控制的使用策略	应开发和实现用于保护信息的密码控制使用策略。	华为云制定并实施密码算法应用规范，规定了密码算法的选择规则及应用规则，同时给出了常见应用实例指导。
A.10.1.2	密钥管理	应制定和实现贯穿其全生命周期的密钥使用、保护和生存期策略。	华为云制定并实施密钥管理安全规范，对密钥生命周期各阶段的安全进行管理。

- **A.11 物理和环境安全**

物理和环境安全目标为设立安全区域，防止对组织信息和信息处理设施的未授权物理访问、损坏和干扰。以及保护设备资产，防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。

编号	控制域	控制措施	华为云的回应
A.11.1.1	物理安全边界	应定义安全边界来保护包含敏感或关键信息和信息处理设施的区域。	华为云信息安全环境采用分区管理，分别定义各区物理环境场地设施（包括门禁、安全岗、摄像监控等）及设备出入控制（包括拍照摄影设备、存储介质等）的不同要求。同时制定并实施各区之间的数据流转策略及访问控制策略。 华为云数据中心严格管理人员及设备进出，在数据中心园区及建筑的门口设置7*24小时保安人员进行登记盘查，限制并监控来访人员授权活动范围。在不同的区域采取不同安全策略的门禁控制系统，严格审核人员出入权限。
A.11.1.2	物理入口控制	安全区域应由适合的入口控制所保护，以确保只有授权的人员才允许访问。	同A.11.1.1
A.11.1.3	办公室、房间和设施的安全保护	应为办公室、房间和设施设计并采取物理安全措施。	同A.11.1.1

A.11.1.4	外部和环境威胁的安全防护	应设计和应用物理保护以防自然灾难、恶意攻击和意外。	在物理保护方面，华为云设立了分区防护。对于可能的自然灾害制定了选址策略以消减风险。对于入侵、授权等风险，建立了监控机制及响应机制。 华为云数据中心会考虑在政治稳定、社会犯罪率低、地理环境友好的地区选址，远离洪水、飓风、地震等自然灾害隐患区域，避开强电磁场干扰，并对于周围的隐患区域设定了最小距离的技术要求。
A.11.1.5	在安全区域工作	应设计和应用安全区域工作规程。	同A.11.1.1
A.11.1.6	交接区	访问点（例如交接区）和未授权人员可进入的其他点应加以控制，如果可能，应与信息处理设施隔离，以避免未授权访问。	华为云通过门禁控制系统，严格审核人员出入权限。华为云要求来访者必须由内部人员全程陪同，并且只能在一般限制区域活动。 华为云对于生产及非生产环境使用物理和逻辑隔离手段。 在数据中心设计施工和运营时，合理划分了机房物理区域（包括高度敏感区域），合理布置了信息系统的组件，以防范物理和环境潜在危险。
A.11.2.1	设备安置和保护	应安置或保护设备，以减少由环境威胁和危险所造成的各种风险以及未授权访问的机会。	华为云制定了机要设备与介质管理相关规定，对设备的安置、保护、进出等均做出要求并制定操作流程。 数据中心的重要配件，由仓储系统中的专门电子加密保险箱存放，且由专人进行保险箱的开关。数据中心的任何配件，都必须提供授权工单方能领取，且领取时须在仓储管理系统中登记。由专人定期对所有物理访问设备和仓储系统物资进行综合盘点追踪。机房管理员不但开展例行安检，而且不定期审计数据中心访问记录，确保非授权人员不可访问数据中心。

A. 11.2.2	支持性设施	应保护设备使其免于由支持性设施的失效而引起的电源故障和其他中断。	华为云对电气、消防安全执行严格管控。华为云数据中心采用多级保护方案保障业务7*24小时持续运行，日常电力供应采用来自不同变电站的双路市电供电。配备柴油发电机，在市电断电时可启动柴油机供电，以备不时之需。并配备了不间断电源(UPS)，提供短期备用电力供应。华为云数据中心建筑防火等级均按一级设计施工，使用了A级防火材料，满足国家消防规范。采用了阻燃、耐火电缆，在管内或线槽铺设，并设置了漏电检测装置。部署了自动报警和自动灭火系统，能够迅速准确发现并通报火情。自动报警系统与供电、监控、通风设备联动，即使意外情况造成无人值守，也能开启自动灭火系统得以控制火情。
A. 11.2.3	布缆安全	应保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听、干扰或损坏。	华为云数据中心选址时会考虑避开强电磁场干扰。华为云机房建设时规定用于任何网络布线和外接设备必须使用安全的导管和防篡改硬件。光纤电缆等通信设备穿过公开访问的区域时，管道和桥架会设置为金属材质，全程覆盖保护电缆，在管内或线槽铺设，并设置了漏电检测装置。
A. 11.2.4	设备维护	设备应予以正确地维护，以确保其持续的可用性和完整性。	对于数据中心的维护，华为云建立了数据中心运维管理相关的制度与流程，其中包含设备的具体管控措施、例行的维护计划等。
A. 11.2.5	资产的移动	设备、信息或软件在授权之前不应带出组织场所。	华为云制定了存储介质及设备进出机房管理规定，要求存储介质及设备进出机房前需进行登记并得到授权。 物理存储介质进出机房时均会进行数据防泄漏管理，并对数据擦除、报废清退流程进行规定，减少可能存在的数据泄露损失。

A.11.2.6	组织场所外设备与资产安全	应对组织场所外的设备采取安全措施，要考虑工作在组织场所以外的不同风险。	华为云制定并实施办公计算机安全管理规定，明确办公资产使用人有义务确保所使用资产的安全，并对使用状况负责。员工携带办公便携机外出时将其随身携带或妥善存放，确保便携机中所存储华为信息的安全。如办公计算机丢失或被盗，员工将及时报告。
A.11.2.7	设备的安全处置或再利用	包含储存介质的设备的所有部分应进行核查，以确保在处置或再利用之前，任何敏感信息和注册软件已被删除或安全地重写。	华为云使用包含存储介质的设备由专人管理，使用完毕后由专人对其进行格式化处理。存储公司保密信息的存储介质报废时由专人确保其上存储的信息均被清除且不可恢复，处理方式包括消磁、物理销毁或低级格式化。
A.11.2.8	无人值守的用户设备	用户应确保无人值守的用户设备有适当的保护。	华为云制定并实施办公场所安全管理规定，对员工的安全责任与行为规范提出要求，制定政策和程序并实施访问控制，确保无人值守的用户设备有适当的保护。
A.11.2.9	清理桌面和屏幕策略	应针对纸质和可移动存储介质，采取清理桌面策略；应针对信息处理设施，采用清理屏幕策略。	华为云制定并实施办公场所安全管理规定，对员工的安全责任与行为规范提出要求，制定政策和程序确保无人值守的工作区没有公开可见的敏感的文档。同时通过意识教育普及、宣传活动开展、BCG及承诺书签署三个方面开展安全意识教育。

- **A.12 运行安全**

运行安全目标包括确保正确、安全地运行信息处理设施，确保信息和信息处理设施防范恶意软件，使用备份防止数据丢失，通过日志和监视程序记录事态并生成证据，运行软件控制以确保运行系统的完整性，防止对技术脆弱性的利用以及执行信息系统审计时考虑将运行系统审计活动的影响最小化。

编号	控制域	控制措施	华为云的回应
A.12.1.1	文件化的操作规程	操作规程应形成文件，并对所需用户可用。	华为云制定了文档化的信息安全政策和程序，为信息处理和通信设施相关的操作提供指导。员工可根据授权查看已发布的信息安全政策和程序。

A. 12.1.2	变更管理	应控制影响组织信息安全的变更，包括组织、业务过程、信息处理设施和系统变更。	华为云建立了系统的变更管理、服务上线流程，并将其要求传达给所有相关的开发人员（包含内部员工及外部合作伙伴），新上线或变更的服务遵循华为云发布、变更管理流程的规定。 员工及其他第三方在状态发生变化后，如离职或职位变更后，按照调动、离职安全审查清单，对内部调离、离职人员进行离岗安全审查，包括离岗权限账号的清理或修改等。
A. 12.1.3	容量管理	应对资源的使用进行监视，调整和预测未来的容量需求，以确保所需的系统性能。	华为云建立了完善的资源管理机制，对于华为统一虚拟化平台中的资源进行容量规划，避免资源被过度使用，满足容量需求。同时收集云服务的组件容量信息、系统性能以监控平台的稳定运营。
A. 12.1.4	开发、测试和运行环境的分离	应分离开发、测试和运行环境，以降低对运行环境未授权访问或变更的风险。	华为云对于生产及非生产环境使用物理和逻辑控制并用的隔离手段，提升面对外部入侵和内部违规操作的自我保护和容错恢复能力，降低对运行环境未授权访问或变更的风险。

A. 12.2.1	恶意软件的控制	应实施检测、预防和恢复控制以防范恶意软件，并结合适当的用户意识教育。	华为云使用IPS入侵防御系统、**Web应用防火墙（WAF - Web Application Firewall）**、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；防病毒软件提供病毒防护及Windows系统内的防火墙；HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。 华为云对员工的安全意识教育在员工在职期间持续进行，有专门的信息安全意识培训计划，意识教育的内容包括防范恶意软件。
A. 12.3.1	信息备份	应按照既定的备份策略，对信息、软件和系统镜像进行备份，并定期测试。	华为云支持在一个数据中心的多个节点内复制存放用户数据。单个节点一旦出现故障，用户数据不会丢失，系统可以做到自动检测和自愈。 单个区域内不同可用区之间，通过高速光纤实现数据中心互联（DCI – Data Center Interconnect），满足跨可用区数据复制基本要求，用户可根据业务需求选择灾备复制服务。 华为云除了提供高可用基础设施、冗余数据备份、可用区灾备等外，还制定了业务连续性计划，并定期对其进行测试。

A.12.4.1	事态日志	应产生、保持并定期评审记录用户活动、异常、错误和信息安全事态的事态日志。	华为云有集中、完整的日志大数据分析系统。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，以确保支撑网络安全事件回溯和合规。该日志分析系统有强大的数据保存及查询能力，确保所有日志保存时间超过180天，90天内可以实时查询。华为云有专门的内审部门，定期对运维流程各项活动进行审计。
A.12.4.2	日志信息的保护	记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。	同A.12.4.1
A.12.4.3	管理员和操作员日志	系统管理员和系统操作员活动应记入日志，并对日志进行保护和定期评审。	同A.12.4.1
A.12.4.4	时钟同步	一个组织或安全域内的所有相关信息处理设施的时钟，应与单一一个基准的时间源同步。	华为云使用标准协议对系统内的时间进行同步。
A.12.5.1	运行系统的软件安装	应实现运行系统软件安装控制规程。	华为云基于严进宽用的原则，保障开源及第三方软件的安全引入和使用。华为云对引入的开源及第三方软件制定了明确的安全要求和完善的流程控制方案，在选型分析、安全测试、代码安全、风险扫描、法务审核、软件申请、软件安装、软件退出等环节，均实施严格的管控。
A.12.6.1	技术方面脆弱性的管理	应及时获取在用的信息系统的技术方面的脆弱性信息，评价组织对这些脆弱性的暴露状况并采取适当的措施来应对相关风险。	华为云建立了专门的漏洞响应团队，及时评估并分析漏洞的原因、威胁程度及制定补救措施，评估补救方案的可行性和有效性。 华为云在其官网公布已经发现的产品或服务的漏洞并进行预警，客户可查看**安全公告**以了解漏洞影响的范围，处置方式及威胁级别。

A. 12.6.2	软件安装限制	应建立并实现控制用户安装软件的规则。	华为云制定并实施桌面终端服务软件标准，办公计算机只使用其中定义的标准操作系统和软件。
A. 12.7.1	信息系统审计的控制	涉及运行系统验证的审计要求和活动，应谨慎地加以规划并取得批准，以便最小化业务过程的中断。	华为云制定并实施渗透测试和漏洞扫描管理规定，其中定义了风险规避策略。在时间选择上，对于系统影响较大的渗透测试和扫描活动须避开业务繁忙时段、重大活动日期以及突发保障时间。同时制定了分层分级策略，包括不对目标进行大规模并发扫描，分批分时进行并控制产生的数据流量，在扫描时先选取业务相对不重要的服务器，确认无风险再扫描其它系统。

- **A.13 通信安全**

通信安全目标包括在网络安全管理中确保网络中的信息及其支持性的信息处理设施得到保护，以及维护在组织内及与外部实体间传输信息的安全。

编号	**控制域**	**控制措施**	**华为云的回应**
A. 13.1.1	网络控制	应管理和控制网络以保护系统中和应用中的信息。	华为云数据中心节点众多、功能区域复杂。为了简化网络安全设计，阻止网络攻击在华为云中的扩散，最小化攻击影响，华为云参考ITU E.408安全区域的划分原则并结合业界网络安全的优秀实践，对华为云网络进行安全区域、业务层面的划分和隔离。安全区域内部的节点具有相同的安全等级。华为云从网络架构设计、设备选型配置到运行维护诸方面综合考虑，对承载网络采用各种针对物理和虚拟网络的多层安全隔离，接入控制和边界防护技术，同时严格执行相应的管控措施，确保华为云安全。

A. 13.1.2	网络服务的安全	所有网络服务的安全机制、服务级别和管理要求应予以确定并包括在网络服务协议中，无论这些服务是由内部提供的还是外包的。	华为云在与网络服务提供商签订的协议中定义了网络服务的安全机制、服务级别SLA和管理要求。
A. 13.1.3	网络中的隔离	应在网络中隔离信息服务、用户及信息系统。	华为云根据业务功能和网络安全风险等级将数据中心划分为多个安全区域，使用物理和逻辑控制并用的隔离手段，提升网络面对入侵和内部威胁的分区自我保护和容错恢复能力。 华为云数据中心主要分为以下五个重要安全区域：DMZ区、公共服务区（Public Service）、资源交付区（POD – Point of Delivery）、数据存储区（OBS – Object - Based Storage）、运维管理区（OM – Operations Management）。 除了上述网络分区，华为云也对不同区域的安全级别进行了划分，根据不同的业务功能，确定不同的攻击面以及不同的安全风险，比如说直接暴露在互联网的区域，安全风险最高，而与互联网几乎没有交互并且不向其他区域开放接口的OM区，攻击面最小，安全风险相对容易控制。 关于安全区域的详细介绍可参考**《华为云安全白皮书》**。
A. 13.2.1	信息传输策略和规程	应有正式的传输策略、规程和控制，以保护通过使用各种类型通信设施进行的信息传输。	华为云已制定相关安全管理规定，定义了信息传输策略和流程，并详细定义了控制要求。

A. 13.2.2	信息传输协议	协议应解决组织与外部方之间业务信息的安全传输。	对于华为云平台客户端到服务端、服务端之间的数据通过公共信息通道进行传输的场景，传输中数据的保护通过如下方式提供： **虚拟专用网络（VPN）**：VPN用于在远端网络和VPC之间建立一条符合行业标准的安全加密通信隧道，将已有数据中心无缝扩展到华为云上，为客户提供端到端的数据传输机密性保障。通过VPN在传统数据中心与VPC之间建立通信隧道，客户可方便地使用华为云的云服务器、块存储等资源，通过将应用程序转移到云中、启动额外的Web服务器来增加网络的计算容量，实现了企业的混合云架构的同时，也降低了企业核心数据非法扩散的风险。 目前，华为云采用硬件实现IKE（密钥交换协议）和IPSec VPN结合的方法对数据传输通道进行加密，确保传输安全。 **应用层TLS与证书管理**：华为云服务提供REST和Highway方式进行数据传输：REST网络通道是将服务以标RESTful的形式向外发布，调用端直接使用HTTP客户端，通过标准RESTful形式对API进行调用，实现数据传输；Highway通道是高性能私有协议通道，在有特殊性能需求场景时可选用。上述两种数据传输方式均支持使用传输层安全协议（TLS – Transport Layer Security）1.2版本进行加密传输，同时也支持基于X.509证书的目标网站身份认证。**证书管理服务（SSL Certificate Service）**则是华为云联合全球知名数字证书服务机构，为客户提供的一站式X.509证书的全生命周期管理服务，实现目标网站的可信身份认证与安全数据传输。

A. 13.2.3	电子消息发送	应适当保护包含在电子消息发送中的信息。	华为云对包含在电子消息中发送的信息进行保护，保护措施包括使用办公计算机安全软件、网络接入管控、权限管理、访问控制、传输加密和内容加密等。
A. 13.2.4	保密或不泄露协议	应识别、定期评审和文件化反映组织信息保护需要的保密性或不泄露协议的要求。	华为云对信息保密以及保密协议签署和存档进行规定，对于员工及外部方须签订的保密协议模板定期进行更新。

- **A.14 系统获取、开发和维护**

信息系统安全要求目标为确保信息安全是信息系统整个生命周期中的一个有机组成部分，包括提供公共网络服务的信息系统的要求。开发和支持过程中的安全目标为确保信息安全在信息系统开发生命周期中得到设计和实现，同时确保用于测试的数据得到保护。

编号	**控制域**	**控制措施**	**华为云的回应**
A. 14.1.1	信息安全要求分析和说明	新建信息系统或增强现有信息系统的要求中应包括信息安全相关要求。	华为云通过完善的制度和流程以及自动化的平台和工具，对软硬件全生命周期进行端到端的管理，全生命周期包括安全需求分析、安全设计、安全编码和测试、安全验收和发布、漏洞管理等环节。 华为云及相关云服务遵从安全及隐私设计原则和规范、法律法规要求，在安全需求分析和设计阶段根据业务场景、数据流图、组网模型进行威胁分析。 当识别出威胁后，设计工程师会根据削减库、安全设计方案库制定消减措施，并完成对应的安全方案设计。所有的威胁消减措施最终都将转换为安全需求、安全功能，并根据公司的测试用例库完成安全测试用例的设计，确保落地，最终保障产品、服务的安全。

A.14.1.2	公共网络上应用服务的安全保护	应保护在公共网络上的应用服务中的信息以防止欺诈行为、合同纠纷以及未经授权的泄露和修改。	华为云对在公共网络上提供的应用服务采用多种安全措施保护其中涉及的数据。包括使用IAM进行访问控制，对用户进行身份认证和鉴权。在信息传输过程中使用安全加密信道（如HTTPS），对存储的静态数据使用安全加密算法进行加密保护，确保不同状态下的数据的机密性。使用数字签名和时间戳等控制机制，防止数据传输过程中被篡改，确保信息完整性并防止重放攻击。对应用服务中的操作留存日志以支持审计。对接口进行身份认证及鉴权、传输保护和边界防护，确保API应用安全。
A.14.1.3	应用服务事务的保护	应保护应用服务事务中的信息，以防止不完整的传输、错误路由、未授权的消息变更、未授权的泄露、未授权的消息复制或重放。	同A.14.1.2
A.14.2.1	安全的开发策略	针对组织内的开发，应建立软件和系统开发规则并应用。	通过结合华为在安全上的长期积累和华为云的现状，华为云不仅积极推行快速迭代的全新DevOps流程，还将华为的安全生命周期SDL无缝嵌入DevOps逐步形成高度自动化的DevSecOps全新安全生命周期管理流程，以及确保全新流程顺利而灵活执行的云安全工程能力和工具链。
A.14.2.2	系统变更控制规程	应使用正式的变更控制规程来控制开发生命周期内的系统变更。	华为云建立了系统的变更管理、服务上线流程，并将其要求传达给所有相关的开发人员（包含内部员工及外部合作伙伴），新上线或变更的服务应遵循华为云发布、变更管理流程的规定。

A. 14.2.3	运行平台变更后对应用的技术评审	当运行平台发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行和安全没有负面影响。	华为云制定了变更管理的管理规定和变更流程，各项变更均需通过多个环节的审核，需通过类生产环境测试、灰色发布、蓝绿部署等方式进行充分验证，确保变更委员会清晰地了解变更动作、时长、变更失败的回退动作以及所有可能的影响，变更委员会审批通过后才可以上线。
A. 14.2.4	软件包变更的限制	应不鼓励对软件包进行修改，仅限于必要的变更，且对所有变更加以严格控制。	同A.14.2.3
A. 14.2.5	系统安全工程原则	应建立、文件化和维护系统安全工程原则，并应用到任何信息系统实现工作中。	华为云制定了公有云云服务质量要求，其中包含安全设计规范集，对系统安全工程原则进行定义并将其应用到服务设计中。
A. 14.2.6	安全的开发环境	组织应针对覆盖系统开发生命周期的系统开发和集成活动，建立安全开发环境，并予以适当保护。	华为云推行快速迭代的全DevOps流程，将华为云的安全生命周期SDL嵌入DevOps逐步形成高度自动化的DevSecOps全新安全生命周期管理流程，以及确保全新流程顺利而灵活执行的云安全工程能力和工具链。 华为云研发环境采取分级管理，对开发环境进行包括物理隔离、逻辑隔离、接入访问控制、数据传输通道审批及审计等保护措施。
A. 14.2.7	外包开发	组织应督导和监视外包系统开发活动。	华为云对研发外包管理提出明确要求，并将外包人员及外包项目的监督纳入员工及项目日常职责中。

A. 14.2.8	系统安全测试	应在开发过程中进行安全功能测试。	华为云所有云服务发布前都经过了多轮安全测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例等。详细内容可参考《华为云安全白皮书》。同时，华为云将其深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具，如SecureCat可以对业界主流的OS和DB的安全配置进行检查。
A. 14.2.9	系统验收测试	应建立对新的信息系统、升级及新版本的验收测试方案和相关准则。	同A.14.2.8
A. 14.3.1	测试数据的保护	测试数据应认真地加以选择、保护和控制。	华为云对测试数据的选择和保护制定了规范，并在测试工作中严格遵循。

- **A.15 供应商关系**

供应商关系中的信息安全目标为确保供应商可访问的组织资产得到保护，供应商服务交付管理目标为维持与供应商协议一致的信息安全和服务交付的商定级别。

编号	控制域	控制措施	华为云的回应
A. 15.1.1	供应商关系的信息安全策略	为降低供应商访问组织资产的相关风险，应与供应商就信息安全要求达成一致，并形成文件。	华为云已建立供应商选择和监督体系，通过合同签订前的尽职调查以及合同签订后的定期评估来管理供应商对华为云具体的要求和合同义务的符合性。
A. 15.1.2	在供应商协议中强调安全	应与每个可能访问、处理、存储、传递组织信息或为组织信息提供IT基础设施组件的供应商建立所有相关的信息安全要求，并达成一致。	供应商安全和隐私要求包含在已签署的合同协议中。与第三方的业务对接人员负责管理他们的第三方关系，包括资产保护要求和供应商对相关应用程序的访问。华为云法务团队也会定期对合同的条款进行审查。
A. 15.1.3	信息与通信技术供应链	供应商协议应包括信息与通信技术服务以及产品供应链相关的信息安全风险处理要求。	华为云在引入供应商时会与其签署保密及服务水平协议，协议中包含对于供应商的安全和隐私数据处理的要求。

A.15.2.1	供应商服务的监视和评审	组织应定期监视、评审和审核供应商服务交付。	同A.15.1.1
A.15.2.2	供应商服务的变更管理	应管理供应商所提供服务的变更，包括维护和改进现有的信息安全策略、规程和控制，管理应考虑变更涉及到的业务信息、系统和过程的关键程度及风险的再评估。	华为云已制定综合采购变更管理规定及流程，按照管理规定严格管理供应商服务的变更。 华为云的灾备策略中规定对于同一服务须使用多家供应商以应对突发事件，以此保留一定的冗余性，维持服务的连续性。

- **A.16 信息安全事件管理**

信息安全事件的管理和改进目标为确保采用一致和有效的方法对信息安全事件进行管理，包括对安全事态和弱点的沟通。

编号	控制域	控制措施	华为云的回应
A.16.1.1	责任和规程	应建立管理责任和规程，以确保快速、有效和有序地响应信息安全事件。	华为云内部制定了安全事件管理机制，包括通用的安全事件响应计划及流程。并持续优化该机制。安全事件响应流程中清晰定义了在事件响应过程中负责各个活动的角色和职责。华为云日志大数据分析系统具备海量日志快速收集、处理、实时分析的能力，支持与第三方安全信息和事件管理（SIEM – Security Information and Event Management）系统如ArcSight、Splunk对接。该系统统一收集所有物理设备、网络、平台、应用、数据库和安全系统的管理行为日志和各安全产品及组件的威胁检测告警日志，持续的监控和实时分析保证对安全事件的及时发现。此外鉴于安全事件处理的专业性和紧迫性，华为云拥有7*24的专业安全事件响应团队以及对应的安全专家资源池来应对。 华为云根据内部管理的要求，每年对信息安全事件管理程序和流程进行测试，所有的安全事件响应人员，包括后备人员均需参与。

A.16.1.2	报告信息安全事态	应通过适当的管理渠道尽快地报告信息安全事态。	华为云已制定安全事件的定级原则和升级原则，根据安全事件对客户业务的影响程度进行事件定级，并根据安全事件的通报机制启动客户通知流程，将事件通知客户。当发生严重的安全事件，已经或可能对大量客户造成严重影响时，华为云可通过公告在最快的时间内将事件的相关信息通知客户。至少包括事件的描述、起因、影响、华为云已采取的措施、建议客户采取的措施等。在事件解决后，会根据具体情况向客户提供事件报告。
A.16.1.3	报告信息安全弱点	应要求使用组织信息系统和服务的员工和合同方注意并报告任何观察到的或可疑的系统或服务中的信息安全弱点。	华为云通过公司统一开展的年度例行学习、考试和签署活动来传递公司对全员在网络安全领域的要求，提高员工网络安全意识,要求包括员工应报告发现的信息安全弱点。对于其他外部相关人员，华为云与其签署保密协议并进行信息安全培训，其中包含信息安全事件报告责任。 华为云向员工提供了报告信息安全事件的渠道及注意事项。
A.16.1.4	信息安全事态的评估和决策	应评估信息安全事态并决定其是否属于信息安全事件。	华为云已建立安全事件响应团队负责监控和分析告警，评估是否属于信息安全事件。
A.16.1.5	信息安全事件的响应	应按照文件化的规程响应信息安全事件。	同A.16.1.1
A.16.1.6	从信息安全事件中学习	应利用在分析和解决信息安全事件中得到的知识来减少未来事件发生的可能性和影响。	华为云有专业的安全事件管理系统，用于记录和跟踪所有的信息安全事件的进展、处置措施与落实，对事件处置后的影响进行分析，对安全事件进行端到端的跟踪闭环，保证整个处置过程可回溯。
A.16.1.7	证据的收集	组织应确定和应用规程来识别、收集、获取和保存可用作证据的信息。	华为云制定了安全事件应急处置流程及响应流程，当服务器/应用疑似被入侵时，由安全响应人员进行取证分析。

- **A.17 业务连续性管理的信息安全方面**

应将信息安全连续性纳入组织业务连续性管理之中，同时应确保信息处理设施的可用性。

编号	控制域	控制措施	华为云的回应
A.17.1.1	规划信息安全连续性	组织应确定在不利情况（如危机或灾难）下，对信息安全及信息安全管理连续性的要求。	华为云已经通过ISO 22301业务连续性管理体系标准的认证，在内部建立了业务连续性管理体系并制定了业务连续性计划，其中包含了自然灾害、事故灾害、信息技术风险等突发事件的应对策略与应对流程。
A.17.1.2	实施信息安全连续性	组织应建立、文件化、实现并维护过程、规程和控制，以确保在不利情况下信息安全连续性达到要求的级别。	同A.17.1.1
A.17.1.3	验证、评审和评价信息安全连续性	组织应定期验证已建立和实现的信息安全连续性控制，以确保这些控制在不利情况下是正当和有效的。	华为云安全演练团队定期制定针对不同产品类型（包含基础服务、运营中心、数据中心、组织整体等）以及不同场景的演练，以维护持续性计划的有效性。当华为云的组织及环境发生重大变化时，也会对业务连续性的有效性进行测试。
A.17.2.1	信息处理设施的可用性	信息处理设施应当实现冗余，以满足可用性要求。	华为云部署了数据中心集群采用的多地域（Region）多可用区（AZ）的架构，实现多可用区冗余相连，排除单点故障的风险，保证业务的连续性。同时，华为云还部署了全局负载均衡调度中心，应用在数据中心实现N+1部署，在一个数据中心故障的情况下可以将流量负载均衡到其他中心。

- **A.18 符合性**

符合性的目标为符合法律和合同要求，避免违反与信息安全有关的法律、法规或合同义务以及任何安全要求。通过信息安全评审确保依据组织策略和规程来实现和运行信息安全。

编号	控制域	控制措施	华为云的回应

A. 18.1.1	适用的法律和合同要求的识别	对每一个信息系统和组织而言，所有相关的法律、法规、规章和合同要求，以及为满足这些要求组织所采用的方法，应加以明确地定义、形成文件并保持更新。	华为云设立了专岗同外部各方保持积极的联系，以追踪法律、法规的相关要求变化。当识别到与华为云服务相关的法律、法规，华为云将及时调整内部安全要求和安全控制水平，跟进对法律、法规要求的符合性。
A. 18.1.2	知识产权	应实现适当的规程，以确保在使用具有知识产权的材料和具有所有权的软件产品时，符合法律、法规和合同的要求。	华为云制定并实施桌面终端服务软件标准，办公计算机只使用其中定义的标准操作系统和软件。 合同层面，华为云严格按照与供应商的约定履行合同。
A. 18.1.3	记录的保护	应根据法律、法规、规章、合同和业务要求，对记录进行保护以防其丢失、毁坏、伪造、未授权访问和未授权发布。	华为云制定了数据安全策略及数据安全保护管理规定，采取适当保护措施并严格执行，以保证数据安全。
A. 18.1.4	隐私和个人可识别信息保护	应依照相关的法律、法规和合同条款的要求，以确保隐私和个人可识别信息得到保护。	华为云以全球隐私保护的法律法规为基石，参考业界广泛认可的优秀实践，建设了华为云的隐私保护体系，对隐私和个人可识别信息进行保护。
A. 18.1.5	密码控制规则	密码控制的使用应遵从所有相关的协议、法律和法规。	华为云使用业界普遍认可的强加密算法对平台内数据进行加密，在传输过程中使用加密协议保障数据安全。
A. 18.2.1	信息安全的独立评审	应按照计划的时间间隔或在重大变化发生时，对组织的信息安全管理方法及其实现（如信息安全的控制目标、控制、策略、过程和规程）进行独立评审。	华为云有专门的审计团队定期评估策略、规程及配套措施和指标的符合性和有效性。此外，独立第三方评估机构也提供独立保证，这些评估员通过执行定期安全评估和合规性审计或检查（例如SOC、ISO标准、PCIDSS审计）来评估信息和资源的安全性、完整性、机密性和可用性，从而对风险管理内容/流程进行独立评估。

A. 18.2.2	符合安全策略和标准	管理者应定期评审其责任范围内的信息处理和规程与适当的安全策略、标准和任何其他安全要求的符合性。	同A.18.2.1
A. 18.2.3	技术符合性评审	应定期评审信息系统与组织的信息安全策略和标准的符合性。	华为云每季度都会组织内部与第三方评估机构分别进行对华为云的所有的系统、应用、网络进行漏洞扫描。对于所有获知的安全漏洞信息，华为云将对每个漏洞进行评估分析，制定并落实漏洞修复方案或规避措施，并在修复后对修复情况进行验证，持续跟踪确认风险得到消除或缓解。 华为云每半年都会组织内部以及外部具有一定资质的第三方进行对华为云的所有的系统及应用进行渗透测试，并对渗透测试的结果进行跟进与整改，渗透测试报告及跟进情况会通过内部审计以及外部认证机构核查。

6 华为云助力客户响应 ISO 27001 标准要求

华为云已通过ISO 27001认证并在此基础上为客户提供安全可靠的云服务，但这并不意味着使用华为云的服务则默认满足了ISO 27001的控制要求。若客户希望通过ISO 27001认证，应根据ISO 27001的指导标准和最佳实践建立、实施、维护和持续改进其组织自身信息安全管理体系，并联系第三方独立认证机构对其进行评估。

信息安全管理体系建设需要从管理和技术两方面着手。在管理层面，客户应制定符合自身需求并满足ISO 27001要求的信息安全策略和规程。在技术层面，华为云提供的产品及服务可以针对部分控制域为客户提供帮助，协助解决客户构建自身信息安全管理体系时遇到的问题。

ISO 27001的部分控制域以及可以协助实现该控制域目标的产品清单可参考下表，如需了解产品详情，请前往华为云官网中的**产品页面**。下文将着重介绍部分华为云主打产品如何帮助客户实现ISO 27001控制域中的控制目标。

ISO 27001控制域	可协助实现该控制域目标的产品
A.8 资产管理	**数据安全中心服务DSC**、**企业主机安全服务HSS**、**对象存储服务OBS**
A.9 访问控制	**统一身份认证服务IAM**、**云堡垒机CBH**、**应用信任中心ATC**
A.10 密码	**数据加密服务DEW**
A.12 运行安全	**漏洞扫描服务VSS**、**Web应用防火墙WAF**、**企业主机安全服务HSS**、**云监控服务CES**、**云日志服务LTS**、**数据库安全服务DBSS**、**云审计服务CTS**、**云备份CBR**、**云硬盘EVS**、**镜像服务IMS**、**云服务器备份CSBS**、**对象存储服务OBS**、**专属分布式存储服务DSS**、**弹性文件服务SFS**、**日志分析服务Log**、**容器安全服务CGS**、**消息通知服务SMN**
A.13 通信安全	**虚拟私有云VPC**、**虚拟专用网络VPN**、**Anti-DDoS流量清洗Anti-DDoS**、**DDoS高防AAD**、**SSL证书管理SCM**、**弹性负载均衡ELB**、**云专线DC**、**云连接CC**

A.14 系统获取、开发和维护	软件开发平台DevCloud、云测CloudTest、CloudIDE、API网关APIG、云性能测试服务CPTS、代码检查CodeCheck、发布CloudRelease、移动应用测试MobileAPPTest
A.15 供应商关系	云监控服务CES、应用运维管理服务AOM
A.16 信息安全事件管理	威胁检测服务MTD、管理检测与响应MDR、态势感知SA
A.17 业务连续性管理的信息安全方面	云备份CBR、云服务器备份CSBS、存储容灾服务SDRS
A.18 符合性	等保合规安全解决方案、内容审核-文本、内容审核-图像、内容审核-视频

6.1 A.8 资产管理

客户在建立信息安全管理体系（ISMS）时，应识别其需要保护的信息资产并定义适当的保护责任，确保信息按照其重要程度受到适当水平的保护，并防止存储在介质中的信息遭受未授权的泄露、修改、移除或破坏。

华为云的**数据安全中心服务（DSC - Data Security Center）**是新一代的云原生数据安全平台，可以为客户提供数据分级分类、数据安全风险识别、数据水印溯源、数据脱敏等基础数据安全能力，并通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。

客户也可以通过采用**企业主机安全服务（HSS - Host Security Service）**全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，构建服务器安全体系，以降低当前服务器面临的主要安全风险。客户可通过提供的可视化界面统一查看并管理同一区域内所有主机的防护状态和主机安全风险。

对象存储服务（OBS – Object Storage Service）可存储客户信息资产中的非结构化数据，对象存储服务支持存储对象的生命周期管理，可以协助客户管理其信息资产。此外，对象存储服务中的多重安全防护如SSL传输加密、服务端加密、身份鉴权均可提供对所存储信息的安全保护。

6.2 A.9 访问控制

限制对信息和信息处理设施的访问，确保授权用户对其所需系统和服务的访问，同时阻止未授权访问，是客户实施访问控制的重要目标。

华为云提供的**统一身份认证服务（IAM – Identity and Access Management）**。提供适合企业级组织结构的用户账号管理服务，为用户分配不同的资源及操作权限。用户通过使用访问密钥获得基于统一身份认证服务的认证和鉴权后，以调用API的方式访问华为云资源。统一身份认证服务可以按层次和细粒度授权，保证同一企业客户的不同用户在使用云资源上得到有效管控，避免单个用户误操作等原因导致整个云服务的不可用，确保客户业务的持续性。

统一身份认证服务支持基于用户组的权限管理机制，支持设定符合客户条件的密码策略、密码更改周期、登陆策略、账号锁定策略、账号停用策略及会话超时策略，提供基于IP的ACL。统一身份认证服务还提供并默认启动多因子认证用以增强账号安全性。

如客户有安全可靠的外部身份认证服务（如LDAP或Kerberos）验证用户的身份并且该外部服务支持SAML 2.0协议，用户可以基于SAML协议登录华为云服务控制台或者通过API方式访问云资源。

云堡垒机（CBH - Cloud Bastion Host）是华为云的一款4A统一安全管控平台，可帮助客户实现集中的帐号、授权、认证和审计管理。云堡垒机提供云计算安全管控的系统和组件，集单点登录、统一资产管理、多终端访问协议、文件传输、会话协同等功能于一体。客户可以通过统一运维登录入口实现对服务器、云主机、数据库、应用系统等云上资源的集中管理和运维审计。客户员工登录公司系统、运维人员访问运维网络区域、员工从企业外部网络远程接入相关资源以及管理员接入管理平台等场景都可以使用云堡垒机实现访问控制及统一操作日志审计，确保网络和网络服务仅由已获授权的用户访问。

6.3 A.10 密码

客户应确保适当和有效地使用密码技术以保护信息的保密性、真实性和完整性。

客户可使用华为云提供的**数据加密服务（DEW - Data Encryption Workshop）**进行专属加密、密钥管理及密钥对管理，数据加密服务支持密钥创建、授权、自动轮换以及密钥硬件保护。客户可根据需要选择所需的密钥管理机制。

华为云提供不同厂商、不同规格（标准加密算法、国密算法等）、不同强度的云硬件安全模块（HSM）供客户选择，满足不同客户的实际需求。云硬件安全模块采用双机部署，保证高可靠性和高可用性。

客户可以使用密钥管理服务（KMS）为可识别的所有者绑定密钥。密钥管理服务中所有密钥均由云硬件安全模块的硬件真随机数生成器生成，保证密钥的随机性。密钥管理服务的根密钥保存在云硬件安全模块中，确保根密钥不泄露。密钥管理服务主机均使用标准的加密传输模式与密钥管理服务服务节点建立安全通信链接，保证密钥管理服务相关数据在节点间的传输安全。密钥管理服务基于**统一身份认证服务（IAM – Identity and Access Management）**中角色统一进行RBAC访问控制。对于用户，只有通过身份验证及密钥管理服务鉴权并拥有密钥操作权限，才能操作密钥管理服务中存储的主密钥。仅设置了只读权限的用户只能查询主密钥信息，不能对主密钥进行操作。密钥管理服务对主密钥进行了客户隔离，每一个租户只能访问与管理属于自己的主密钥，无法操作其他租户的主密钥。此外，系统管理员仅有设备管理权限，没有任何访问主密钥的权限。

6.4 A.12 运行安全

客户的运行安全目标包括确保安全地运行信息处理设施、防范恶意软件、使用备份以防止数据丢失、通过日志和监视程序记录事态并生成证据、运行软件控制以确保运行系统的完整性、防止对技术脆弱性的利用以及执行信息系统审计时考虑将运行系统审计活动的影响最小化等。华为云为客户提供了多种云服务以协助实现这些运行安全目标。

客户可通过华为云提供**漏洞扫描服务（VSS - Vulnerability Scan Service）**。实现对Web应用、操作系统、配置基线的扫描，以及对资产内容合规检测和弱密码检测，以识别网站或服务器暴露在网络中的安全风险。华为云会第一时间针对紧急爆发的通用漏洞CVE进行分析并更新规则，提供快速、专业的CVE漏洞扫描。客户可通过部署**Web应用防火墙（WAF - Web Application Firewall）**对网站业务流量进行多维度检测和防护。Web应用防火墙可结合深度机器学习智能识别恶意请求特征和防御未知威胁，通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫

扫描、跨站请求伪造等攻击，全面避免网站被黑客恶意攻击和入侵，保护Web服务安全稳定。针对主机安全防护，华为云的**企业主机安全服务（HSS - Host Security Service）**可实现对主机系统的全面安全评估，评估后通过将现有系统存在的账户、端口、软件漏洞、弱口令风险进行展示，提示客户进行加固，消除安全隐患，提升主机整体的安全性。企业主机安全服务还提供入侵检测功能，在发现账户暴力破解、进程异常、异常登陆等事件后快速进行告警，客户可通过事件管理全面了解告警事件，帮助客户及时发现资产中的安全威胁、实施掌握资产的安全状态，使用入侵检测技术检测和防止入侵网络。

华为云提供的**云监控服务（CES - Cloud Eye Service）**可帮助客户实时监控服务器的运行状态以及云上资源的使用情况，当出现硬件故障时，云监控将会通过邮件、短信、HTTP/S通知客户。华为云提供的**云日志服务（LTS – Log Tank Service）**提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，包括对虚拟机的配置、日志的更改等，便于查询与追踪。结合云监控服务，客户可以对用户登录日志进行实时监控，当遇到恶意登陆行为可触发告警并拒绝该IP地址的请求。同时云日志服务及**数据库安全服务（DBSS - Database Security Service）**都可对系统组件的日志进行记录并保存，供客户进行日志审核。华为云的**云审计服务 (CTS - Cloud Trace Service)**可以实时、系统地记录用户通过云账户登录管理控制台执行的操作。客户可根据企业对日志保留期限的要求购买不同规格的对象存储服务服务以实现日志的备份。

如果客户需要对业务数据、软件和系统镜像进行备份，华为云提供了多种有不同侧重的产品和服务。例如，客户可以使用华为云提供的**云备份（CBR - Cloud Backup and Recovery）**服务对云内的云服务器、云硬盘、文件服务，云下文件、VMware虚拟化环境进行备份，在发生病毒入侵、人为误删除、软硬件故障等导致数据不可用的场景前可将数据恢复到任意备份点。客户可使用**云硬盘（EVS - Elastic Volume Service）**中的快照功能，当数据丢失时，可通过快照将数据完整的恢复到快照时间点。华为云还为客户提供了**镜像服务（IMS - Image Management Service）**，客户可使用该产品对云服务器的实例进行备份，当实例的软件环境出现故障时使用备份的镜像进行恢复。**云服务器备份（CSBS - Cloud Server Backup Service）**服务可同时为云服务器下多个云硬盘创建一致性在线备份，保护数据安全可靠，降低数据被非法篡改的风险。作为能够实现多种数据存储场景的**对象存储服务（OBS - Object Storage Service）**，客户也可将其用于企业数据备份/归档。

6.5 A.13 通信安全

客户的通信安全目标包括保护网络中的信息及信息处理设施，以及维护在组织内及与外部实体间传输信息的安全。

华为云为客户提供的**虚拟私有云（VPC - Virtual Private Cloud）**服务可为租户构建隔离且私密的虚拟网络环境，在流畅访问的同时隔离租户，在此基础上支持灵活配置虚拟私有云之间的互联互通。客户可以完全掌控自己的虚拟网络构建与配置，包括虚拟私有云内的IP地址段、子网、安全组等子服务，并通过配置网络ACL和安全组规则，对进出子网和虚拟机的网络流量进行严格的管控，满足客户更细粒度的网络隔离需求。客户可将虚拟私有云用于划分网络区域、在云上建立隔离的生产与测试环境等。

对于需要将已有数据中心扩展到华为云上的场景，客户可以使用**虚拟专用网络（VPN - Virtual Private Network）**。该服务可用于在传统数据中心与华为云提供的虚拟私有云之间建立安全加密通信隧道，便于客户使用云平台中的云服务器、块存储等资源，将应用程序转移到云中、启动额外的Web服务器、增加网络的计算容量等，实现企业的混合云架构。

为了保证构建安全的网络防护体系，客户除了通过网络技术和网络设备实现安全域划分之外，还可以通过华为云提供的一系列安全服务来提高网络边界防护能力，例如，

客户可通过**Anti-DDoS流量清洗**服务实现对网络层和应用层的DDoS攻击防护，Anti-DDoS为客户提供精细化的防护服务，客户可以根据业务的应用类型，配置流量阈值参数，并通过实时告警功能查看攻击和防御状态。客户如需更大流量攻击的检测和清洗服务，可通过华为云的**DDoS高防（AAD - Advanced Anti-DDoS）**服务来实现。

华为云的**SSL证书管理(SCM - SSL Certificate Manager)**服务可以向客户提供一站式证书的全生命周期管理，实现网站的可信身份认证与安全数据传输。平台联合全球知名数字证书服务机构为用户提供购买SSL证书的功能，用户也可以将本地的外部SSL证书上传到平台，实现用户对内部和外部SSL证书的统一管理。客户在部署该服务后，可以将服务使用的HTTP协议替换成HTTPS协议以消除HTTP协议的安全隐患。该服务可应用于网站可信认证、应用可信认证以及应用数据传输保护。

6.6 A.14 系统获取、开发和维护

客户应将信息安全融入信息系统生命周期，确保信息安全在信息系统开发生命周期中得到设计和实现。

软件开发平台（DevCloud）是华为云面向开发者提供的一站式云端DevOps平台。帮助客户在云端进行项目管理、代码托管、流水线、代码检查、编译构建、部署、测试、发布等，让开发者快速便捷地在云端进行开发。使用DevCloud开放的API和调用示例，客户可以对项目、工作项、成员、代码仓库、流水线等进行管理。通过合理配置**云开发环境服务（CloudIDE）**，客户可以实现安全开发环境的建立和保护。软件开发平台提供的一站式测试解决方案**云测（CloudTest）**可以满足客户执行系统安全测试及系统验收测试的需求。

软件开发平台支持云上开发，提供可视化、可定制的自动交付流水线帮助实现云端可持续交付，同时覆盖软件交付的全生命周期，提供软件研发端到端支持，全面支撑客户落地DevOps。软件开发平台增加多重安全防护功能，保证核心资产安全。客户可以将自身的安全生命周期嵌入软件开发平台，形成自动化的DevSecOps安全生命周期管理流程，确保信息安全在开发生命周期中得到设计和实现。

API网关（APIG - API Gateway）是华为云提供的高性能、高可用、高安全的API托管服务，可以从两方面帮助客户，作为API提供者，客户可以将成熟的业务能力（如服务、数据等）作为后端服务，在API网关中开放API，并通过线下方式提供给API调用者使用，或者发布到API市场，实现业务能力变现。作为API调用者，客户可以获取并调用API提供者在API网关开放的API，减少开发时间与成本。API网关支持API生命周期管理、版本管理、创建环境变量、流量控制、监控告警等，同时提供安全防护组件如访问控制和签名密钥，可以帮助客户控制访问API的IP地址和帐户，以及保障API网关请求的后端服务的安全，防止服务中的信息遭到未经授权的泄露和修改。

6.7 A.15 供应商关系

在供应商关系这一控制域中，客户主要的信息安全目标是保证供应商的信息安全级别和服务交付质量。

客户可通过华为云提供的**云监控服务（CES - Cloud Eye Service）**实现对**弹性云服务器（ECS - Elastic Cloud Server）**的使用量以及网络带宽的立体化监控，云监控服务支持通过Open API、SDK、Agent方式上报租户自定义的指标，并通过邮件、短信等方式进行通知，以保证客户第一时间知悉业务运行情况。

应用运维管理服务（AOM - Application Operations Management）是云上应用的一站式立体化运维管理平台，实时监控应用及云资源，采集各项指标、日志及事件等数据分析应用健康状态，提供告警及数据可视化功能，帮助客户及时发现故障，全面掌握应用、资源及业务的实时运行状况。

6.8 A.16 信息安全事件管理

客户在信息安全事件管理中的信息安全目标为按照既定方法对信息安全事件进行管理，包括对安全事态和弱点的沟通、信息安全事件响应流程以及对事件的总结分析。

威胁检测服务（MTD - Managed Threat Detection）是一种持续监控访客对客户使用的全局服务的帐号/域名的恶意活动和未经授权行为的服务。此服务集成了AI智能引擎、威胁情报、规则基线三种检测方式，智能检测来自多个云服务日志数据中的访问行为以发现是否存在潜在威胁，对可能存在威胁的访问行为生成告警信息，输出告警结果。帮助客户在威胁未形成巨大风险之前及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护客户的帐户安全，保障服务稳定运行，提升运维效率。

客户也可以使用**管理检测与响应（MDR - Managed Detection and Response）**服务，该服务可以帮助客户建立由管理、技术与运维构成的安全风险管控体系，结合企业与机构业务的安全需求反馈和防控效果对安全防护进行持续改进，帮助企业与机构实现对安全风险与安全事件的有效监控，并及时采取有效措施持续降低安全风险并消除安全事件带来的损失。

态势感知（SA - Situation Awareness）是华为云为客户提供的安全管理与态势分析平台。能够检测出包括DDoS攻击、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等多种云上安全风险。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为客户呈现出全局安全攻击态势，帮助客户识别、收集及获取信息安全事件相关证据并通过分析事件以减少事件在未来发生的可能性和影响。同时态势感知可以关联**DDoS高防**、**企业主机安全服务**、**Web应用防火墙**和**数据库安全服务**等，集中呈现安全防护状态。

6.9 A.17 业务连续性管理的信息安全方面

客户应将信息安全连续性纳入组织业务连续性管理之中，同时应确保信息处理设施的可用性。

客户可以使用华为云提供的**云备份（CBR – Cloud Backup and Recovery）**服务实现对**云硬盘（EVS - Elastic Volume Service）**、**弹性云服务器（ECS - Elastic Cloud Server）**和**裸金属服务器（BMS - Bare Metal Server）**的备份保护。云备份支持基于快照技术的备份服务以及利用备份数据恢复服务器和云硬盘的数据。同时云备份支持同步线下备份软件BCManager中的备份数据以及对备份数据的完整性校验。

客户如需创建在线备份，可以使用**云服务器备份（CSBS - Cloud Server Backup Service）**服务，它可以为云服务器下所有云硬盘创建一致性在线备份，当发生病毒入侵、人为误删除、软硬件故障时将数据恢复到任意备份点。云服务器备份提供对弹性云服务器和裸金属服务器的备份保护服务，支持基于多云硬盘一致性快照技术的备份服务，并支持利用备份数据恢复服务器数据，最大限度保障用户数据的安全性和正确性，确保业务安全。

为满足组织在灾难发生时对信息安全及信息安全管理连续性的要求，华为云向客户提供**存储容灾服务（SDRS - Storage Disaster Recovery Service）**为弹性云服务器、云硬盘和**专属分布式存储（DSS - Dedicated Distributed Storage Service）**等服务提供容灾与灾难恢复。存储容灾服务通过存储复制、数据冗余和缓存加速等多项技术，提供给用户高级别的数据可靠性以及业务连续性。存储容灾服务有助于保护业务应用，将弹性云服务器的数据、配置信息复制到容灾站点，并允许业务应用所在的服务器停机期间从另外的位置启动并正常运行，从而提升业务连续性。

6.10 A.18 符合性

客户应开展合规工作，确保符合适用的法律、法规和合同要求。

华为云依托自身安全能力与安全合规生态，为客户提供了**等保合规安全解决方案**。该服务是一款包括定级备案、差距分析、规划设计、整改加固、等保测评、安全保障全流程闭环的一站式服务。可以帮助客户快速、低成本完成安全整改，满足等保合规需求。

7 结语

华为云始终秉持着华为公司“以客户为中心”的核心价值观，积极践行信息安全实践，为此华为云构建了信息安全管理体系，应用业界通用的信息安全保护技术，通过第三方机构的认证与审核检查安全控制的有效落实，致力于保护客户的数据安全。

同时，为帮助客户应对日益复杂和开放的网络环境及日益发展的信息安全技术，华为云不断开发各种数据保护领域的工具、服务和方案，支持客户提升数据保护能力，降低风险。

本白皮书仅供客户作为参考，不具备任何法律效力或构成法律建议，也不作为任何客户在云上环境一定合规的依据。客户应酌情评估自身业务和安全需求，选用适合的云产品及服务。

8 引用资料

《GB/T 22080-2016/ISO/IEC 27001：2013 信息技术 安全技术 信息安全管理体系 要求》

9 版本历史

日期	版本	描述
2021年7月	1.0	首次发布