华为云中华人民共和国香港特别行政区证券及期货行业监管遵从性指南

文档版本 1.0

发布日期 2022-05-16

HUAWEI

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

1.1 背景与发布目的

在科技发展的浪潮中，越来越多的金融机构在逐渐寻求业务转型并希望借助先进的技术以降低成本、提升运营效率、实现业务模式的创新。中华人民共和国香港特别行政区（下文简称“中国香港”）证券及期货事务监察委员会（The Securities and Futures Commission，简称SFC）是一个独立的法定机构，负责监管中国香港的证券和期货市场。为了规范证券及期货行业对于信息科技的运用，SFC发布了一系列监管要求和指南，针对获准从事证券及期货相关受规管活动的机构或组织（持牌法团，Licensed corporation，简称LC）在科技风险管理及网络安全、外间电子数据储存的使用、互联网交易安全管理等方面提出了相关监管要求。

华为云作为云服务供应商，致力于协助证券及期货客户满足这些监管要求，持续为证券及期货客户提供遵从证券及期货行业标准要求的云服务及业务运行环境。本文将针对中国香港证券及期货在使用云服务时通常需遵循的监管要求和指南，详细阐述华为云将如何协助其满足监管要求。

1.2 适用的中国香港证券及期货监管要求简介

- **外间电子数据储存的使用（Use of external electronic data storage）**：该政策文件规定了关于持牌法团将其监管纪录存放于电子数据储存供应商（external electronic data storage provider，简称EDSP）的监管要求，阐释了有关纪录备存的批准规定，以及持牌法团在使用电子数据储存供应商以电子方式存放或处理数据时须遵循的监管标准。
- **降低及纾减与互联网交易相关的黑客入侵风险指引（Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading）**：该政策文件规定了有关降低或纾减与互联网交易相关的黑客入侵风险的基本要求。本政策文件订明的监控措施仅可降低或纾减与互联网交易相关的黑客入侵风险，无法完全消除有关风险。必须强调的是，该等监控措施只是持牌法团应达致的最低标准，并非详尽无遗。
- **有关资讯科技风险管理及网络保安的良好业界作业方式（Good industry practices for IT risk management and cybersecurity）**：该政策文件规定了一份关于科技风险管理和网络保安的的行业实践清单，从事互联网交易的持牌法团可考虑将当中所列的良好作业方式纳入其信息科技及网络保安风险管理框架内。

该份清单是根据过往发出的通函所提议的监控措施，并辅以外部网络保安专家参照最新的科技发展所提供的建议所编制。

1.3 名词定义

- **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。

- **证监会**

  指中国香港证券及期货事务监察委员会（The Securities and Futures Commission，SFC ）。

- **电子数据储存供应商（EDSP）**

  包括以下各项的外间供应商：

  - 公共及私有云端服务；
  - 设于传统数据中心的数据储存服务器或装置；
  - 电子数据的其他虚拟储存形式；及
  - 某些科技服务，而(i)在使用这些服务期间会产生数据，且数据会储存于有关科技服务供货商或其他数据储存供货商，及(ii)该等科技服务供货商可将所产生和储存的数据检索出来。

- **互联网交易**

  透过持牌人或注册人以互联网为基础的交易设施向该持牌人或注册人传送交易指示的安排。

- **客户内容数据**

  客户使用华为云服务过程中存储或处理的内容，包括但不限于数据、文件、软件、图像、音频、视频等类型的数据。

2 华为云的认证情况

华为云继承了华为公司完备的管理体系以及IT系统的建设和运营经验，对华为云各项服务的集成、运营及维护进行主动管理，并持续改进。截至目前，华为云已获得众多国际和行业安全合规资质认证，全力保障客户部署业务的安全，主要包括：

全球性标准类认证

认证	描述
ISO 20000-1:2011	ISO 20000是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的IT服务来满足客户和业务的需求。
ISO 27001:2013	ISO 27001是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，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。
ISO 27017:2015	ISO 27017是针对云计算信息安全的国际认证。ISO 27017的通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。
ISO 22301:2012	ISO 22301是国际公认的业务连续性管理体系标准，通过对风险的识别、分析和预警来帮助组织规避潜在事件的发生，并且制定完备的“业务连续性计划”，有效地应对中断发生后的快速恢复，保持核心功能正常运行，将损失和恢复成本降至最低。
SOC审计	SOC审计报告是由第三方审计机构根据美国注册会计师协会（AICPA）制定的相关准则，针对外包服务商的系统和内部控制情况出具的独立审计报告。
PCI DSS认证	支付卡行业数据安全标准（PCI DSS）是由JCB、美国运通、Discover、万事达和Visa等五家国际信用卡组织共同建立的一套支付卡行业数据安全标准，由支付卡行业安全标准委员会管理。它是世界上最权威、最严格的金融机构认证。

认证	描述
CSA STAR金牌认证	CSA STAR认证是由标准研发机构BSI（英国标准协会）和CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。
国际通用准则CC EAL3+	CC(Common Criteria)认证是一种信息技术产品和系统安全性的评估标准，它提供了一组通用的安全功能要求和安全保证要求，并在这些保证要求的基础上提供衡量IT安全性的尺度（即评估保证级EAL），使得独立的安全评估结果可以互相比较。
ISO 27018:2014	ISO 27018是专注于云中个人数据保护的国际行为准则。ISO 27018的通过，表明华为云已满足国际认可的公有云个人数据保护措施的要求，可保证客户个人数据安全。
ISO 29151:2017	ISO 29151是国际个人身份信息保护实践指南。ISO 29151的通过，表明华为云实施国际认可的个人数据处理的全生命周期的管理措施。
ISO 27701:2019	ISO 27701规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。华为云通过ISO27701表明了其在个人数据保护具有健全的体制。
BS 10012:2017	BS 10012是BSI发布的个人信息数据管理体系标准，BS10012认证的通过表明华为云在个人数据保护上拥有完整的体系以保证个人数据安全。
M&O认证	Uptime Institute是目前全球公认的数据中心标准化组织和权威的专业认证机构。华为云数据中心已获得Uptime Institute颁发的全球顶级数据中心基础设施运维认证(M&O认证)。获得M&O认证象征着华为云数据中心运维管理已处于国际领先水平。
NIST网络安全框架(CSF)	NIST CSF由标准、指南和管理网络安全相关风险的最佳实践三部分组成，其核心内容可以概括为经典的IPDRR能力模型，即风险识别能力（Identify）、安全防御能力（Protect）、安全检测能力（Detect）、安全响应能力（Response）和安全恢复能力（Recovery）五大能力。
PCI 3DS认证	PCI 3DS标准，旨在保护执行特定3DS功能或者存储3DS数据的3DS环境，支持3DS的实施。PCI 3DS的评估对象为3D协议执行环境，包括访问控制服务器、目录服务器或3DS服务器功能；以及3D执行环境内和连接到环境所需要的系统组件，如防火墙、虚拟服务器、网络设备、应用等；除此之外，还会评估3D协议执行环境的过程、流程、人员管理等。

地区性标准类认证

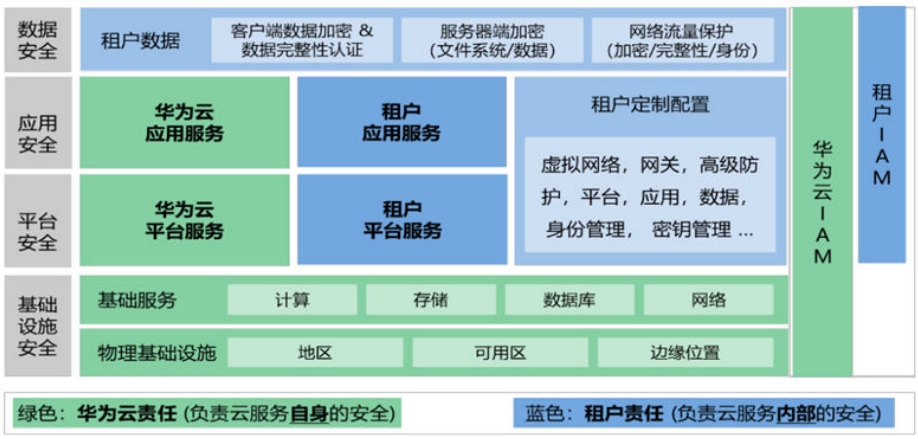
认证	描述
网络安全等级保护	网络安全等级保护是中国公安部用于指导国内各组织单位进行网络安全建设的依据，目前已成为各行业广泛遵守的通用安全标准。华为云通过了网络安全等级保护三级，关键Region、节点通过了网络安全等级保护四级。
新加坡 MTCS Level 3 认证	MTCS多层云计算安全规范是由新加坡信息技术标准委员会制定的标准。该标准要求CSP在云计算中采用健全的风险管理和安全实践。目前华为云新加坡大区获得MTCS最高安全评级的Level 3等级认证。
可信云金牌运维专项评估	金牌运维评估是面向已通过可信云服务认证的云服务供应商的运维能力专项评估。华为云通过“金牌运维”评估，体现了华为云服务具备完善、健全的运维管理体系，符合国内权威云服务运营和维护保障要求的认证标准。
云服务用户数据保护能力认证	云服务用户数据保护能力评估是针对云服务用户数据安全的评估机制，评测关键指标范围包括事前防范、事中保护、事后追溯三个层面。
工信部云计算服务能力 评估	云计算服务能力评估是以《信息技术云计算云服务运营通用要求》等相关国家标准为依据的分级评估标准。华为私有云和公有云双双获得云计算服务能力“一级”符合性证书。
可信云评估	可信云评估是由数据中心联盟（DCA）组织、中国信息通信研究院（工信部电信研究院）测评的面向云计算服务和产品的权威评估。
网信办网络安全审查	网信办网络安全审查是中央网信办依据国家标准《云计算服务安全能力要求》进行的第三方安全审查。华为云服务政务云平台顺利通过该安全审查（增强级），表明华为政务云平台在安全性、可控性等方面获国家网络安全管理机构的认可。

关于更多华为云的安全合规信息以及获取相关合规证书，可参见华为云官网“**信任中心-合规中心**”。

3 华为云安全责任共担模型

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，需要租户与华为云共同努力。基于此，华为云为帮助租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。在模型中租户与华为云具体负责的区域可参见下图。

图 3-1 责任共担模型



基于责任共担模型，华为云与租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。

租户：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租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租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。

关于华为云与租户的安全责任详情，可参考华为云已发布的**《华为云安全白皮书》**。

4 华为云全球基础设施

华为云目前已陆续在全球多个国家或地区开服。华为云的基础设施采用在全球部署多个地理区域（Region）和多可用区（AZ）的模式，华为云能够在多个地理区域内或同一地域内多个可用区之间灵活替换计算实例和存储数据，每个可用区都是一个独立故障维护域，也就是各可用区物理上是隔离的。用户可充分利用这些地理区域和可用区，规划应用系统在云上的部署和运行。基于多个可用区进行应用的分布式部署，可保证在大多故障情况下系统都能连续运行。关于更多关于华为云基础设施的信息，参见华为云官网“**全球基础设施**”。

5 华为云如何遵从及协助客户满足 SFC《外间电子数据储存的使用》的要求

中国香港证券及期货事务监察委员会于2019年10月31日发布了《外间电子数据储存的使用》。该规定从有关将监管纪录只存放于电子数据储存供应商时适用的规定、批准将处所用作存放监管纪录、使用外间数据储存或处理服务的持牌法团的一般责任等领域提出对持牌法团外间电子数据储存的使用相关要求。

持牌法团在遵循《外间电子数据储存的使用》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《外间电子数据储存的使用》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助持牌法团满足这些控制要求。

5.1 有关将监管纪录只存放于电子数据储存供应商时适用的规定

原文编号	控制域	具体控制要求	华为云的应答
7(a)(b)	电子数据储存供应商	若持牌法团希望将任何监管纪录只存放于电子数据储存供应商，便应确保遵从以下规定： （a）该电子数据储存供应商（i）是在中国香港成立为法团的公司或根据《公司条例》（第622章）注册的非中国香港公司，而在这两种情况下均由在中国香港进行营运的人员担当职员，及 （ii）借位于中国香港的数据中心向持牌法团提供数据储存（中国香港电子数据储存供应商）。此外，只存放于该电子数据储存供应商的持牌法团的监管纪录将会在法律或法规所规定须存放有关监管纪录的整个期间内，时刻存放于该数据中心。 （b）作为另一选择，若该电子数据储存供应商并非第7（a）段所界定的中国香港电子数据储存供应商，持牌法团必须取得该电子数据储存供应商有关按证监会可能提出的要求而提供监管纪录和协助的承诺（参考本通函附录1所载模板的形式。）	若要将监管记录存放于EDSP，客户应确认EDSP是否满足左述7（a）条件。若不满足，客户应取得EDSP有关按证监会可能提出的要求而提供监管纪录和协助的承诺。华为云作为云服务提供商，也是在中国香港的EDSP，为LC客户提供数据存储服务。华为云以区域为单位提供服务，区域也即是客户内容数据的存储位置，华为云未经授权绝不会跨区域移动客户的内容数据。客户在使用云服务时，依据就近接入原则、不同地域的适用的法律法规要求等进行区域的选择，确保客户内容数据存储在目标位置。华为云在中国香港设立了数据中心，以供客户在中国香港本地来存储和处理他们的数据。 为方便客户遵守该政策，并根据《证券及期货条例》第130条获得SFC对该等申请的批准，华为云可应客户的要求，使用通函附录1中的模板，提供一份已签署的承诺书。同时，在签发已签署的承诺书之前，客户需要使用通函附录2中的模板向华为云提供一份通知书副本。通知书旨在授权并要求华为云作为EDSP向SFC提供相关监管记录。

原文编号	控制域	具体控制要求	华为云的应答
7(C)	电子数据储存供应商	（c）持牌法团应只将监管纪录存放于适当和可靠的电子数据储存供应商，及已顾及到该电子数据储存供应商的运营能力、技术专业知识及财政稳健性。	客户在选择EDSP时，应考虑其运营能力、技术专业知识及财政稳健性。作为EDSP，华为云在运营能力、技术能力、财务稳健性方面的情况如下： **（1）运营能力：**华为云遵循ISO27001、ISO20000、ISO22301等国际标准建立信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，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。 **（2）技术能力：**华为云用在线提供云服务的方式，将华为30多年在ICT基础设施领域的技术积累和产品解决方案开放给客户。华为云具备全栈全场景AI、多元架构、极致性能、安全可靠、开放创新五大核心技术优势。比如，在AI领域，华为云AI已在城市、制造、物流、互联网、医疗、园区等10大行业的300+个项目进行落地。在多元架构方面，华为云打造了基于X86+鲲鹏+昇腾的多元算力云服务新架构，让各种应用跑在最合适的算力之上，实现客户价值最大化。 **（3）财务稳健性：**华为云是华为的云服务品牌，自2017年正式上线以来,华为云一直处于快速发展中，收入保持强劲增长态势。全球权威咨询机构Gartner发布的《Market Share: IT Services, worldwide 2019》报告显示，华为云全球IaaS市场排名第六，中国市场排名前三，全球增速最快，高达222.2%。

原文编号	控制域	具体控制要求	华为云的应答
7(d)(f)	监管记录的取览	（d）持牌法团应确保其只存放于某电子数据储存供应商的所有监管纪录，全部可应证监会要求在没有不当延误的情况下被取览，及可从该持牌法团就这个目的而根据《证券及期货条例》第130条获批准的中国香港处所以可阅读形式重现。 （f）不论持牌法团使用哪一家电子数据储存供应商，及其使用的电子数据储存供应商在何处设置储存数据的硬件，持牌法团应顾及所有在任何有关司法管辖区的相关政治及法律问题，确保证监会在履行职能或行使权力时对监管纪录的有效取览，不会因监管纪录的存放方式而被削弱或不当地延误。	客户如果将监管记录只存放于EDSP,应采取一定措施保障监管机构对监管记录的取览权。为配合客户满足监管要求，华为云作为EDSP： **（1）**华为云不用客户数据做商业变现，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守适用的法律法规或政府机关的约束性命令，并严格遵守《个人资料（私隐）条例》所述的数据保护原则。 **（2）**客户对其存储在云环境中的内容拥有完全所有权。客户有责任确保其内容以清晰易读的形式保存，并确保数据的完整性。为使客户能够遵守相关要求，客户可以考虑将监管记录存储在华为云的**对象存储服务（OBS）**中。OBS是一个基于对象的海量存储服务，为租户提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删桶、上传、下载、删除对象等。OBS为用户提供超大存储容量，可存放任意类型的文件，适合普通用户、网站、企业和开发者使用。OBS支持对象限时访问和跨域资源共享（CORS），对象限时访问功能提供一个自定义时长的有效URL，可用于匿名用户软件下载或其他应用程序访问，跨域资源共享功能允许配置跨域共享策略，支持第三方请求访问OBS中的资源。通过这两个功能，客户可按照要求将监管记录提供给监管机构进行取览。

原文编号	控制域	具体控制要求	华为云的应答
7(e)	稽查线索资料的记录和保存	（e）该持牌法团应确保， （i）若其储存于电子数据储存供应商的监管纪录曾被取览（包括阅读、编写及修改），其能够就此提供以可阅读形式显示的详细稽查线索资料，及 （ii）稽查线索完整记录持牌法团对任何储存于电子数据储存供应商的监管纪录的取览。稽查线索资料应在持牌法团须存放监管纪录的期间内一直存放。持牌法团应被限制只能以只读方式取览稽查线索资料，并且应确保每名曾取览监管纪录的用户都能够从稽查线索中被独特地识别出来。	客户应对监管记录的取览进行完整地记录，以提供可阅读形式显示的详细稽查线索资料。客户还应确保稽查线索资料的存放时间不短于监管记录的存放时间，并且只能以可读权限取览稽查线索资料。为配合客户满足监管要求，华为云作为EDSP： **（1）**客户可以考虑将监管记录存储在华为云的**对象存储服务（OBS）**中。OBS支持对桶的访问请求，并保存访问日志记录，用于进行请求分析或日志审计。通过访问日志记录，客户作为桶的所有者，可以深入分析访问该桶的用户请求性质、类型或趋势。当用户开启一个桶的日志管理功能后，OBS会自动对该桶的访问请求进行日志记录，并生成日志文件，写入用户指定的桶（即目标桶）中。 **（2）**华为云的**云审计服务（CTS）**为客户提供包括OBS在内的云服务资源的操作记录，供用户查询、审计和回溯使用。客户可在CTS中查询OBS的访问日志，方便客户监控OBS的读、写、删除等操作，测量OBS访问统计数据，跟踪异常，定位问题。授权用户帐户对存储桶的访问可以从带有时间戳的日志中识别出来。CTS支持将操作记录合并，周期性地生成事件文件，实时同步转存至OBS存储桶，帮助用户实现操作记录高可用、低成本的长久保存。

5.2 使用外间数据储存或处理服务的持牌法团的一般责任

原文编号	控制域	具体控制要求	华为云的应答
12	尽职调查	持牌法团应对电子数据储存供应商及与其提供数据储存服务的基础设施、人员及程序有关的监控措施，进行适当的初步尽职审查，以及定期监察电子数据储存供应商的服务交付，初步尽职审查与定期监察需与电子数据储存供应商的服务的关键程度、重要性、规模及范围相称。有关的尽职审查应涵盖： （a）电子数据储存供应商的内部管治，以保护持牌法团的监管纪录（当监管纪录是存放在电子数据储存供应商内的情况下），以及可能包括评价储存设备的实体保安、寄存的类别（即是否为专用或共享硬件）、网络基础设施的保安、信息技术系统及应用系统、身份及取览的管理、网络风险管理、信息保安、数据遗失及违规通知、鉴证能力、灾难恢复及业务持续运作程序；及 （b）由电子数据储存供应商就储存持牌法团的监管纪录而作出的任何分包安排，特别是关于网络风险管理及信息保安。	客户应对EDSP进行尽职调研，并定期监察EDSP的服务交付。尽职调查应涵盖物理安全、网络安全、灾难恢复及业务连续性、分包管理等方面。华为云作为EDSP，在上述方面的情况如下： **（1）物理安全：**华为云已制定并实施了物理和环境安全防护策略、规程和措施，满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3+标准。数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问，而且提供了合理足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，华为云运维运营团队定期对全球的数据中心执行风险评估，保证数据中心严格执行访问控制、安保措施、例行监控审计、应急响应等措施。 **（2）数据隔离：**华为云承载了众多客户的数据，各服务产品和组件从设计之初就规划并实现了合理隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性，服务设计的实现则因服务而异。如块存储，数据隔离以卷（云硬盘）为单位进行，每个卷都关联了一个客户标识，挂载该卷的虚拟机也必须具有同样的客户标识，方能完成卷的挂载，助力客户数据隔离。 **（3）网络安全能力：**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ITUE.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

原文编号	控制域	具体控制要求	华为云的应答
			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提高华为云安全。 **（4）风险管理：**华为云遵从华为公司的信息安全风险管理框架，对风险管理范围、风险管理组织以及风险管理过程中的标准进行了严格定义。华为云每年进行一次风险评估，并且在信息系统发生重大变更、公司业务发生重大变化或适用的法律法规、标准发生重大变化时，华为云会进行相应风险评估。 **（5）信息安全：**华为云参照ISO27001构建了完善的信息安全管理体系，制定了华为云整体的信息安全策略，其中明确了信息安全管理组织的架构与职责，信息安全体系文件的管理办法，以及信息安全的重点关注方向和目标，包括：资产安全、访问控制、密码学、物理安全、操作安全、通信安全、系统开发安全、供应商管理、信息安全事件管理、以及业务连续性。全方位保护客户系统和数据的保密性、完整性和可用性。 **（6）灾难恢复及业务连续性：**为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得IS022301认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。 **（7）分包管理：**为配合客户行使对电子数据储存供应商的监管，华为云线上的**《华为云用户协议》**对客户和华为云的安全职责进行划分，华为云**《华为云服务等级协议》**规定了华为云提供的服务水平。同时，华为云也制定了线下合同模板，可根据客户的具体要求，在其中规定华为云若聘用分包商，需通知客户，并对分包的服务负责。华为云制定了自身的供应商管理机制，从供应商的产品和供应商本身的内部管理都提出了安全需求。

原文编号	控制域	具体控制要求	华为云的应答
			此外，华为云会对供应商进行定期的稽核。此外会与涉及网络安全的供应商签署网络安全协议，在服务过程也中会持续监控其服务质量并对供应商进行绩效评分，对安全绩效差的供应商进行合作降级处理。 **（8）身份及取览的管理：**请参见本文档**5.1**下**“监管记录的取览”**和**“稽查线索资料的记录和保存”**，以及**5.2**下**“访问控制”**的相关内容。 **（9）数据遗失及违规通知：**请参见本文档**6.3**下**“网络保安事故报告”**的相关内容。 **更多信息请参见《华为云安全白皮书》**以及本文档的其他章节。
14	数据加密	持牌法团亦应采取适当的措施，确保电子数据储存供应商能够保护属于机密的有关数据，以防止在蓄意或不慎的情况下披露予未经授权的第三方或被他们所误用。为保护其属于机密的有关数据，持牌法团应在数据静止及传递时将其加密，或制订有效的程序和机制，保障其保密性及安全性。当有关数据被加密时，持牌法团须实施适当的密码匙管理监控措施，持续管有加密及解密匙。	客户应制定有效的程序和机制，保障存储在EDSP的数据的保密性和安全性。若对有关数据进行加密，客户应实施适当的密钥管理机制。作为EDSP，华为云的**云硬盘（EVS）**、**对象存储服务（OBS）**、**镜像服务（IMS）**和关系型数据库等多个服务均提供数据加密（服务端加密）功能供客户选择，这些服务都采用高强度的算法对存储的数据进行加密。另外，华为云为客户提供了**数据加密服务（DEW）**的密钥管理功能，可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，助力客户云上数据的安全。DEW采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为客户创建和管理密钥，HSM 拥有 FIPS 140-2（2级和3级）的主流国际安全认证，助力用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法获取客户根密钥。DEW还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。更多信息请参见**《华为云安全白皮书》**6.8.2数据加密（DEW）服务。

原文编号	控制域	具体控制要求	华为云的应答
15	访问控制	持牌法团应实施适当的政策、程序及监控措施，以管理用户的取览权，确保有关数据只可由获授权的人员就恰当的目的而作出更改，及免受损害或窜改。一般来说，应禁止不同用户之间共享系统验证码（例如密码），以确保每名曾取览监管纪录的用户都能够被独特地识别出来。	客户应制定用户账号和权限管理机制，为每个员工分配唯一可辨别身份的账号，并确保员工对数据的访问经过合理授权。作为EDSP： （1）华为云的**统一身份认证服务（IAM）**为客户提供云上资源访问控制。使用IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户协同操作资源时，使用IAM可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来助力用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过**云审计服务（CTS）**作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。 （2）华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对运维人员进行身份认证，如USB key、Smart Card 等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度审计。
16	数据的机密性	若持牌法团只是将有关数据的一部分存放在电子数据储存供应商内（不论是否因数据敏感顾虑或其他原因），持牌法团便应制定监控措施，防止有关数据在未经妥善授权的情况下迁移至电子数据储存供应商。	客户应制定监控措施，防止有关数据在未经合理授权的情况下迁移至EDSP。作为EDSP： （1）华为云不用客户数据做商业变现，在用户协议中明确表明不会访问或者使用用户的内容，除非是为用户提供必要的服务，或者为遵守适用的法律法规或政府机关的约束性命令，并严格遵守《个人资料（私隐）条例》所述的数据保护原则。 （2）华为云各服务产品和组件从设计之初就规划并实现了隔离机制，避免客户间有意或无意的非授权访问、篡改等行为，降低数据泄露风险。以数据存储为例，华为云的块存储、对象存储、文件存储等服务均将客户数据隔离作为重要特性。

原文编号	控制域	具体控制要求	华为云的应答
17	安全责任划分	不论科技是如何部署的，持牌法团应确保它们清晰界定、明确了解并妥善管理其与电子数据储存供应商之间的责任分配，例如保安设定的配置、工作负载保护及凭证管理。	华为云明确定义了与客户之间的安全责任共担模型，客户可参见本文档3.华为云安全责任共担模型，也可在华为云官网上查阅**《华为云安全白皮书》**中关于责任共担模型的具体内容。
19	业务连续性	若持牌法团在进行其受规管活动时使用外间数据储存或处理服务，则应评价其对服务供应商提供及时和持续不断的服务的依赖程度，以及假如服务中断可能会对持牌法团及其客户带来的运作影响。持牌法团应制订适当的应变计划，确保其在运作方面的抵御能力，以及规定电子数据储存供应商须披露有关数据遗失、违反保安规定，或可能对持牌法团的受规管活动构成重大影响的运作失误的情况。	客户应评估其对EDSP提供持续服务的依赖程度，以及服务中断可能产生的影响。另外，客户还应制定适当的应变计划，并要求EDSP披露可能对客户的受规管活动造成重大影响的安全事件。作为EDSP： **（1）**为向客户提供持续、稳定的云服务，华为云制定了符合自身业务特色的业务连续性管理体系，并已获得IS022301认证。华为云每年会在组织内进行业务连续性的宣传和培训，以及定期做应急演练和测试，持续优化应急响应机制。 **（2）**为配合客户满足事件后通知的要求，华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：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。

原文编号	控制域	具体控制要求	华为云的应答
21	终止协议	持牌法团应与电子数据储存供应商制订具有法律约束力的协议，当中订明合约终止条文。合约条文可能包含要求有关电子数据储存供应商须协助过渡至新电子数据储存供应商，或容许将数据移回该持牌法团的处所内储存，以及在适用的情况下，厘清数据及知识产权于合约终止后的拥有权。	客户应与EDSP签订具有法律约束力的协议，协议中应当明确终止条款，如服务终止的过渡安排、数据及知识产品的归属。作为EDSP： （1）华为云提供了线上的**《华为云用户协议》**以及**《华为云服务等级协议》**，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。 （2）在服务协议终止时，客户可通过华为云提供的**对象存储迁移服务（OMS）**和**主机迁移服务（SMS）**，将内容数据从华为云中迁移出去，如迁移至本地数据中心。

6 华为云如何遵从及协助客户满足 SFC《降低及纾减与互联网交易相关的黑客入侵风险指引》的要求

中国香港证券及期货事务监察委员会于2017年10月27日发布了《降低及纾减与互联网交易相关的黑客入侵风险指引》。该规定从保护客户的互联网交易帐户、基础设施保安管理、网络保安管理及监督等领域提出对持牌法团互联网交易安全管理相关要求。

持牌法团在遵循《降低及纾减与互联网交易相关的黑客入侵风险指引》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《降低及纾减与互联网交易相关的黑客入侵风险指引》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助持牌法团满足这些控制要求。

6.1 保护客户的互联网交易帐户

原文编号	控制域	具体控制要求	华为云的应答
1.4	数据加密	持牌人或注册人应以强效的加密程序： (a)将敏感数据，例如客户登入数据（即用户名称和密码）及交易数据，在内部网络与客户装置之间传输时加密；及 (b)保护储存于其互联网交易系统的客户登入密码。	客户应建立加密管理机制，对敏感数据的存储和传输进行加密。作为云服务提供商，为保障客户安全的处理云上数据，华为云对包括数据存储和数据传输在内的数据生命周期的各阶段进行层层防护。 **（1）数据存储：**目前，**云硬盘（EVS）**、**对象存储服务（OBS）**、**镜像服务（IMS）**和关系型数据库等多个服务均提供数据加密（服务端加密）功能，采用高强度的算法对存储的数据进行加密。服务端加密功能集成了华为云**数据加密服务（DEW）**的密钥管理功能，由DEW进行密钥全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，助力客户云上数据的安全。 **（2）数据传输：**当客户通过互联网提供Web网站业务时，可以使用华为云联合全球知名证书服务商提供的证书管理服务。通过给Web网站申请并配置证书，实现网站的可信身份认证以及基于加密协议的安全传输。针对客户业务混合云部署和全球化布局的场景，可以使用华为云提供的**虚拟专用网络（VPN）**、**云专线（DC）**、**云连接（CC）**等服务，实现不同区域之间业务的互联互通和数据传输安全。

6.2 基础设施保安管理

原文编号	控制域	具体控制要求	华为云的应答
2.1	配置安全的网络基础设施	持牌人或注册人应透过妥善的网络隔离措施（即设有多重防火墙的隔离区）来配置安全的网络基础设施，以保护关键系统（例如互联网交易系统及交收系统）及客户数据免受网络攻击。	客户应制定适当的网络隔离措施来部署网络基础设施，以保护关键系统及客户数据免受网络攻击。为配合客户满足监管要求： **（1）**客户可以使用华为云提供的**虚拟私有云（VPC）**实现不同区域之间网络隔离。VPC可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络ACL和安全组规则，对进出子网以和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。 **（2）**华为云**Web应用防火墙服务（WAF）**是结合了华为多年攻防经验和一系列针对性优化算法的高级Web应用防火墙。采用正则规则和语义分析的双引擎架构对SQL注入、跨站攻击、命令和代码注入、目录遍历、扫描器、恶意bot、webshell、CC等攻击实现实时的高性能防护。华为云WAF给用户提供简便的管理界面，用户可根据自身业务需要进行相关防护设置，亦可在集中的管理界面上查看防护日志并对误报的事件进行处理。 **（3）**华为云建立了合理、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；Anti-DDoS 快速发现和防护DDoS 攻击；WAF实时检测和防御Web 攻击；IDS/IPS实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。

原文编号	控制域	具体控制要求	华为云的应答
2.2	使用者接达管理	持牌人或注册人应设有政策及程序，以确保只容许有需要的人士接达或使用系统。此外，持牌人或注册人应至少每年检视使用者有权接达的关键系统（例如互联网交易系统及交收系统）及数据库（例如客户数据）的列表，以确保只有获核准且有需要的人士方可接达或使用系统。	客户应制定用户账号和权限管理机制，确保员工对系统的访问和使用经过合理授权，并每年对关键系统及数据库的账号和权限进行复核。为配合客户满足监管要求： **（1）**客户可通过华为云的**统一身份认证服务（IAM）**对使用云资源的用户账号进行管理。IAM除了支持密码认证之外还支持多因子认证，客户可自主选择是否启用。如果租户有安全可靠的外部身份认证服务商，可以将IAM服务的联邦认证外部用户映射成华为云的临时用户，并访问租户的华为云资源。IAM 可以按层次和细粒度授权，管理员可以基于用户的工作职责规划使用云资源的权限，还可以通过设置用户访问云服务系统的安全策略，例如设置访问控制列表来限制未信任网络的恶意接入。 此外，华为云的**云审计服务（CTS）**，可提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。 **（2）**为配合客户满足监管要求，华为云内部建立了运维和运营账号管理机制。运维人员接入华为云管理网络对系统进行集中管理时，需使用员工身份账号，且要求使用双因子认证。所有运维账号由LDAP集中管理，通过统一运维审计平台集中监控并进行自动审计。以实现从创建用户、授权、鉴权到权限回收的全流程管理。并根据不同业务维度和相同业务不同职责，实行 RBAC权限管理。保证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。

原文编号	控制域	具体控制要求	华为云的应答
2.4	修补管理	持牌人或注册人应及时监察和评估软件提供者发布的保安修补程序或修正程序，并视乎对影响进行的评估，在切实可行的情况下尽快进行测试，并在测试完成后一个月内执行该等程序。	客户应建立补丁管理机制，持续监控软件提供商补丁的发布情况，并对补丁进行影响评估和测试，在完成测试后及时安装补丁。作为云服务提供商，华为云通过镜像工厂，由专业安全团队对虚拟机操作系统公共镜像进行安全加固，并及时修复系统安全漏洞最终生成安全更新了的公共镜像，并通过**镜像服务（IMS）**持续提供给租户。同时提供相关加固和补丁信息以供用户对镜像进行测试、排除故障及其他运维活动时参考。由客户根据相关应用运行及安全运维策略，选择直接使用最新的公共镜像重新创建虚拟机或自行创建已安装安全补丁的私有镜像。
2.5	端点保护	持牌人或注册人应及时执行和更新防毒及抗恶意软件解决方案（包括相应的定义档案及辨识档案），以侦测关键系统服务器及工作站内的恶意应用程序及恶意软件。	客户应建立防病毒管理机制，执行并更新防病毒解决方案。客户可通过使用华为云的**企业主机安全服务（Host Security Service，简称HSS）**来保护主机安全。企业主机安全服务提供资产管理、漏洞管理、基线检查、恶意程序检测等功能，能够帮助企业更方便地管理主机安全风险，助力实时发现并阻止黑客入侵行为。
2.7	实体保安	持牌人或注册人应订立实体保安政策及程序，以确保关键系统组件（例如系统服务器及网络装置）处于安全的环境下，及防止有人在未经授权的情况下实际接触寄存互联网交易系统及关键系统组件的设施。	客户应制定物理安全管理政策和程序，防止人员在未经授权的情况下接触关键系统基础设施。为配合客户满足监管要求，华为云已制定并实施了物理和环境安全防护策略、规程和措施，满足GB50174《电子信息机房设计规范》A类和TIA942《数据中心机房通信基础设施标准》中的T3+标准。数据中心不但有妥善的选址，在设计施工和运营时，合理划分了机房物理区域，合理布置了信息系统的组件，以防范物理和环境潜在危险（如火灾、电磁泄露等）和非授权访问，而且提供了足够的物理空间、电源容量、网络容量、制冷容量，以满足基础设施快速扩容的需求。同时，华为云运维运营团队定期对全球的数据中心执行风险评估，保证数据中心严格执行访问控制、安保措施、例行监控审计、应急响应等措施。更多关于内容请参见**《华为云安全白皮书》**5.1物理与环境安全。

原文编号	控制域	具体控制要求	华为云的应答
2.8	系统及数据备份	持牌人或注册人应至少每天将其业务纪录、客户及交易数据库、服务器及证明文件在脱机媒体进行备份。 持牌人或注册人亦应采纳适当的恢复方法，使重大系统变更得以成功还原。	客户应建立备份管理机制，定期对重要数据和文件进行备份，并采用适当的备份恢复方案，以便成功回滚重大系统变更。为配合客户满足监管要求： **（1）**华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用**对象存储服务（OBS）**的版本控制、**云硬盘备份（VBS）**、**云服务器备份（CSBS）**等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，保证在灾难发生时数据不丢失。 **（2）**客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵从相关政策前提下自动将客户应用和数据转离受影响区域，保证业务的连续性。华为云还部署了全局负载均衡调度中心，客户的应用在数据中心实现N+1部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。

原文编号	控制域	具体控制要求	华为云的应答
2.9	网络保安情境的应变计划	为确保在网络保安事故发生时可有效执行适当的应变程序，持牌人或注册人应尽一切合理努力，使其业务延续计划及危机管理程序涵盖可能出现的网络攻击情境（例如分布式阻断服务攻击），及业务纪录和客户数据因网络攻击（例如勒索软件）而完全损毁的情况。	客户应制定安全事件响应机制，并制定应对网络攻击的业务连续性计划及危机管理程序。为配合客户满足监管要求： **（1）**华为云内部制定了完善的安全事件管理机制，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。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。华为云使用大数据安全分析系统，关联各种安全设备的告警日志进行统一分析。根据安全事件对客户业务的影响程度进行事件定级，并启动客户通知流程，将事件通知客户。在事件解决后，会根据具体情况向客户提供事件报告。 **（2）**基于云面临环境下存在复杂的安全风险，华为云制定了各类的专项应急预案，每年会对重大的安全风险场景进行应急演练，从而在发生此类安全事件时，快速削减可能产生的安全风险，保障网络韧性。

6.3 网络保安管理及监督

原文编号	控制域	具体控制要求	华为云的应答
3.2	网络保安事故报告	持牌人或注册人应订立书面政策及程序，订明怀疑或确实的网络保安事故应以何种方式上报及向内（例如负责互联网交易的负责人员或主管人员）和向外（例如客户、证监会及其他执法机构（如适用））报告。	客户应制定安全事件的上报机制，明确各类安全事件的上报方式和上报对象。为配合客户满足监管要求，华为云内部制定了完善的事件管理和客户通知通报流程，若华为云底层基础平台发生事件，相关人员将依据流程分析事件的影响，若事件已对或即将对云服务客户产生影响时，华为云将启动通知通报机制，将事件通知客户。通知的内容包括但不限于：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。

原文编号	控制域	具体控制要求	华为云的应答
3.3	内部系统用户的网络保安意识培训	持牌人或注册人应至少每年向所有内部系统用户提供足够的网络保安意识培训。在设计培训课程的内容时，持牌或注册人应顾及其所面对的网络保安风险类别及水平。	客户应建立网络安全培训机制，定期对内部员工进行网络安全意识培训。作为云服务提供商，为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为对全体员工从意识教育普及、宣传活动开展、员工商业行为准则（BCG）及承诺书签署三个方面开展安全意识教育。参考业界优秀实践，华为建立了完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，提升员工能力，向客户交付安全的产品、解决方案与服务。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。更多关于内容请参见**《华为云安全白皮书》**4.4人力资源管理。

7 华为云如何遵从及协助客户满足 SFC《有关资讯科技风险管理及网络保安的良好业界作业方式》的要求

中国香港证券及期货事务监察委员会于2017年10月27日发布了《有关资讯科技风险管理及网络保安的良好业界作业方式》。该规定从安全的系统及网络基础设施、系统接达监控措施及数据保护、保安监察及容量管理、系统开发及变更管理、数据备份及应变计划、供货商管理、提高内部系统用户的网络保安意识等领域提出对持牌法团科技风险及网络保安管理相关要求。

持牌法团在遵循《有关资讯科技风险管理及网络保安的良好业界作业方式》要求时，华为云作为云服务供应商，可能会参与到要求所涉及的部分活动中。以下内容将总结《有关资讯科技风险管理及网络保安的良好业界作业方式》中与云服务供应商相关的控制要求，并阐述华为云作为云服务供应商，会如何帮助持牌法团满足这些控制要求。

7.1 安全的系统及网络基础设施

原文编号	控制域	具体控制要求	华为云的应答
B1	网络隔离	因应各个区域所储存的数据或所连接的系统需要设置的接达管制，将内部网络划分为不同区段；具体而言，监控及保护敏感数据在不同网络区段之间的流动。	客户应对网络进行区段划分，对不同区域的数据或系统连接进行访问控制。客户可以使用华为云提供的**虚拟私有云（VPC）**实现不同区域之间网络隔离。VPC可为租户构建出私有网络环境，实现不同租户间在三层网络的完全隔离，租户可以完全掌控自己的虚拟网络构建与配置，并通过配置网络ACL和安全组规则，对进出子网以和虚拟机的网络流量进行严格的管控，满足租户更细粒度的网络隔离需求。

原文编号	控制域	具体控制要求	华为云的应答
B2-B4	网络基础设施安全	B2.设立隔离区，并采取以下稳健的保安监控措施： -配置不同品牌及种类的多重防火墙，以监控及过滤隔离区与可靠的内部网络之间的网络通讯； -实施入侵防御系统、网上应用系统防火墙及对抗进阶持续性威胁的解决方案，以保护隔离区内面向互联网的服务器； -配置入侵检测系统以及系统信息及事件管理解决方案，以侦测及监察未获授权的接达及数据传输； -不在隔离区内储存或缓存客户登入数据等敏感数据；及 -对隔离区内的数据传输进行强效加密，以保护敏感数据。 B3. 对主要的信息科技系统实施保安配置（即系统设定）。停用或移除任何不使用的程序、端口、计算机程序及特权帐户。 B4. 实施应用程序白名单解决方案，以防在用户的计算机或服务器安装未经授权的应用程序。	客户应设立网络隔离区（DMZ），并采取适当的网络安全监控和保护措施，如防火墙、入侵检查系统、Web应用防火墙等。作为云服务提供商，华为云携手云安全商业合作伙伴向租户提供咨询服务，协助租户对虚拟网络，虚拟机（包括虚拟主机和访客虚拟机）的安全配置，系统和数据库安全补丁管理，虚拟网络的防火墙、API网关和高级安全服务的定制配置，DoS/DDoS攻击防范，租户安全事件的应急响应以及灾难恢复。如： **（1）华为云Web应用防火墙服务（WAF）**是结合了华为多年攻防经验和一系列针对性优化算法的高级Web应用防火墙。采用正则规则和语义分析的双引擎架构对SQL注入、跨站攻击、命令和代码注入、目录遍历、扫描器、恶意bot、webshell、CC等攻击实现实时的高性能防护。华为云WAF给用户提供简便的管理界面，用户可根据自身业务需要进行相关防护设置，亦可在集中的管理界面上查看防护日志并对误报的事件进行处理。 **（2）华为云虚拟专用网络（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，为用户提供端到端的数据传输机密性保障。目前，华为云采用硬件实现的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，助力传输安全。 **（3）**客户可通过使用华为云的**企业主机安全服务（HSS）**来保护主机安全。企业主机安全服务提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为。HSS部分功能具体如下： ● **账户破解防护：**检测SSH、RDP、FTP、SQL Server、MySQL等账户遭受的口令破解攻击，对识别出的攻击源IP封锁24小时，禁止其再次登录，防止主机因账户破解被入侵。

原文编号	控制域	具体控制要求	华为云的应答
			• **资产管理：**提供账号、端口、进程、Web目录和软件等安全资产信息的管理和分析。 • **基线检查：**检测系统口令复杂度策略、经典弱口令、风险账号，以及常用系统与中间件的配置，识别不安全项目，预防安全风险。 • **恶意程序检测：**通过程序特征、行为检测，结合AI图像指纹算法以及云查杀，有效识别病毒、木马、后门、蠕虫和挖矿软件等恶意程序，并提供一键隔离查杀能力。
B5	分布式拒绝服务（DDoS）	评估遭受分布式阻断服务攻击的风险，并透过过滤大量及可疑的输入流量／网络攻击（如适用）实施反分布式阻断服务的机制和解决方案。	客户应评估遭受DDoS攻击的风险，并实施有效的防DDoS攻击机制和解决方案。作为云服务供应商，华为云为客户提供两种防DDoS攻击服务：**Anti-DDoS流量清洗服务（简称Anti-DDoS）**和**DDoS高防（Advanced Anti-DDoS，简称AAD）**。Anti-DDoS是一种流量清洗服务，为客户的华为云内资源（弹性云服务器、弹性负载均衡），提供网络层和应用层的DDoS攻击防护，并提供攻击拦截实时告警，有效提升用户带宽利用率，保障业务稳定可靠。AAD则可服务于华为云和非华为云的主机，用户可以通过修改DNS解析或对外服务地址为高防IP，将恶意攻击流量引流到高防IP清洗，助力重要业务不被攻击中断。 华为云的防DDoS攻击服务提供精细化的抵御DDoS攻击的功能，包括但不限于Ping Flood、 SYN Flood、UDP Flood、Challenge Collapsar、HTTP Flood 、DNS Flood。用户只需根据租用带宽及业务模型自助配置防护阈值，系统检测到攻击后就会实时通知用户并进行有效防御。 华为云的防DDoS攻击服务还通过华为云自身的一系列技术，如安全的基础架构平台、安全组网及边界防护、虚拟机网络隔离、API 接口安全与日志审计等，增强其安全能力，保障防DDoS攻击服务服务自身的业务安全。

7.2 系统接达监控措施及数据保护

原文编号	控制域	具体控制要求	华为云的应答
C1、C2、C5	系统的访问控制	C1. 制订有足够制衡的接达管理和特权帐户管理的程序。利用特权或紧急帐户来监控、记录及监察所有接达端点装置、服务器及网络设备的情况。采用身份接达管理及特权接达管理工具，从而确保各项接达管理作业方式得以贯彻落实。 C2. 对特权用户接达操作系统施加限制，以避免安装恶意应用程序、在未经授权下篡改系统配置，或在用户的计算机或服务器移除保安工具。 C5. 在没有高级管理层的书面批准及说明作为凭证的情况下，系统开发人员（包括服务供货商）不得接达实际运作环境。如获允许接达实际运作环境，便须设有机制以记录及监察该等活动。	客户应建立访问控制和特权账号管理程序，对终端、服务器及网络设备的访问进行监控、记录和审计，同时对特权账号的使用进行限制，避免利用特权账号进行非法操作。作为云服务提供商： **（1）**华为云的**统一身份认证服务（IAM）**为客户提供云上资源访问控制。使用IAM，客户管理员可以管理用户账号，并且可以控制这些用户账号对客户名下资源具有的操作权限。当客户企业存在多用户协同操作资源时，使用IAM可以避免与其他用户共享账号密钥，按需为用户分配最小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来助力用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。客户也可通过**云审计服务（CTS）**作为辅助，为租户提供云服务资源的操作记录，供用户查询、审计和回溯使用。 **（2）**华为云的运维人员接入华为云管理网络对系统进行集中管理时，需使用唯一可辨识的员工身份账号，用户账号均配置了强密码安全策略，且密码定期更改，以防止暴力破解密码。华为云还采用双因子认证对云为人员进行身份认证，如 USB key、Smart Card 等。员工账号用于登录 VPN、堡垒机，实现用户登录的深度审计。

原文编号	控制域	具体控制要求	华为云的应答
C3-C4	密码管理	C3. 制订正式的密码匙管理政策及程序，以规管为机密及敏感数据加密的密码匙的生命周期。 C4. 透过采取系统登入密码，实施数据保护监控措施，而登入密码应进行盐值及单向散列加密，最好使用慢散列函数的加密程序。	客户应制定密码管理政策和程序，使用安全的加密算法对机密及敏感数据进行加密，并有效管理密钥的生命周期。为配合客户满足监管要求，华为云提供**数据加密服务（DEW）**，DEW是一个综合的云上数据加密服务。它可以提供专属加密、密钥管理、密钥对管理等功能。通过专属加密服务，用户可以选择基于国家密码局认证或FIPS 140-2第3级验证的硬件加密机，实现高性能、用户独享的加密能力，支持SM1-SM4的国产密钥加密算法。通过密钥管理功能，客户可对密钥进行全生命周期集中管理。在未授权的情况下，除客户外的任何人无法获取密钥对数据进行解密，助力客户云上数据的安全。DEW采用分层密钥管理机制，方便各层密钥的轮换。华为云使用的硬件安全模块（HSM）为客户创建和管理密钥，HSM 拥有 FIPS 140-2（2级和3级）的主流国际安全认证，助力用户的数据合规性要求，能够做到防入侵、防篡改，即使是华为运维人员也无法获取客户根密钥。DEW还支持客户导入自有密钥作为客户主密钥进行统一管理，方便与客户已有业务的无缝集成、对接。同时，华为云采取用户主密钥在线冗余存储、根密钥多份物理离线备份以及定期备份的机制，保障了密钥的持久性。 更多信息请参见**《华为云安全白皮书》**6.8.2数据加密（DEW）服务。

7.3 保安监察及容量管理

原文编号	控制域	具体控制要求	华为云的应答
D2、D5	安全监控与日志管理	D2. 针对各类型的网络攻击，设定行为监控解决方案及其相关参数，以侦测恶意活动（例如监控在正常办公时间后，某些类别的数据如客户标识符、原始码及大量经加密档案的数据外泄）。 D5. 备存及审核计算机或网络系统的稽查纪录 / 接达纪录，以识别任何未经授权的接达尝试或对系统安全的攻击。	客户应采取网络安全监控措施以侦测恶意活动，并对计算机和网络系统的访问和操作记录进行保存和审计。为配合客户满足监管要求： **（1）**华为云建立了稳固、完善的边界和多层立体的安全防护系统。例如，多层防火墙对网络进行区域隔离；Anti-DDoS快速发现和防护DDoS攻击；WAF实时检测和防御Web 攻击；IDS/IPS实时检测和阻断来自互联网的网络攻击、监控主机异常行为等。针对公有云攻击的手段多样、流量巨大的特点，华为云使用态势感知分析系统，关联各种安全设备的告警日志，并统一进行分析，快速全面识别已经发生的攻击，并预判尚未发生的威胁。 **（2）**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，日志包含资源ID(如：源IP、主机ID、用户ID等)、事件类型、日期时间、受影响的数据/组件/资源的ID（如目的IP、主机ID、服务ID等）、成功或失败等信息，以助力支撑网络安全事件回溯。该日志分析系统有强大的数据保存及查询能力，使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。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。

原文编号	控制域	具体控制要求	华为云的应答
D7-D8	性能及容量管理	D7. 设立系统性能警示界线，例如中央处理器用量、内存用量、磁盘读写速度、可用空间及带宽，以监察系统及网络活动。 D8. 实施警示机制，一旦系统性能警示界线被触及，会及时向有关人士通报，以便采取修正行动。	客户应建立性能及容量管理机制，设定系统性能阈值，并进行持续监控和异常响应。为配合客户遵从监管要求，华为云制定了规范的容量管理及资源预测程序，对华为云容量进行统筹管理，提升华为云资源可用性服务水平。根据各方的输入，滚动预测未来资源容量，制定合适的资源扩容方案，并每天定期监控华为云的容量使用情况，分析评估业务容量瓶颈及性能瓶颈，在资源达到预设阈值时，发布资源预警，进而采取进一步解决方法，避免对租户云服务的系统性能造成影响。 同时，华为云的云监控服务**云监控服务（Cloud Eye Service，简称CES）**为用户提供一个针对**弹性云服务器（Elastic Cloud Server，简称ECS）**、带宽等资源的立体化监控平台。云监控服务提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。用户可以自主设置告警规则和通知策略，以便及时了解各服务的实例资源运行状况和性能。

7.4 系统开发及变更管理

原文编号	控制域	具体控制要求	华为云的应答
E1	变更管理	制订正式的系统变更管理程序，并对系统改动、实际运作环境的部署和系统还原实施有效的监控措施。任何预定及紧急的变更 / 修正均应获得管理层书面批准。	客户应制定变更管理程序，对系统变更采取有效的监控措施，要求任何变更都要获得合理的授权方可实施。华为云作为云服务提供商，负责其提供的基础设施和 IaaS、PaaS和SaaS各类各项云服务的变更管理。华为云制定了完善的变更管理流程并定期对其评审和更新。按照变更可能对业务造成影响的程度定义了变更类别和变更窗口，以及变更通告机制。该流程要求所有的变更申请生成后，由变更经理进行变更级别判断后提交给华为云变更委员会，通过评审后方可按计划对现网实施变更。所有的变更在申请前，都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，使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。

原文编号	控制域	具体控制要求	华为云的应答
E2	开发安全管理	在软件开发生命周期强制实行以下保安作业方式，以便在推出新系统或实施主要系统变更之前早日识别及修补保安漏洞： -在系统设计时间考虑保安要求（例如用户认证和授权、登入时段管理、数据完整性、稽查纪录）； -制订安全的程序编制模式； -进行原始码评审，包括同业评审和自动原始码扫描；及 -在系统套用到实际运作环境前进行保安测试。	客户应建立开发安全管理机制来管理软件开发生命周期，包括安全需求分析、安全设计、安全编码、代码评审、安全测试等。作为云服务提供商，华为的开发测试过程均遵循统一的系统（软件）安全开发管理规范，对各个环境的访问进行了严格控制。为配合客户遵从监管要求，华为云通过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。具体如下： **（1）**华为云及相关云服务遵从安全及隐私设计原则和规范、适用的法律法规要求，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削减措施，并完成对应的安全方案设计。所有的威胁削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，保障产品、服务的安全。 **（2）**华为云严格遵从华为公司对内发布的多种编程语言的安全编码规范。使用静态代码扫描工具例行检查，其结果数据进入云服务工具链，以评估编码的质量。所有云服务在发布前，均须完成静态代码扫描的告警清零，有效降低上线时编码相关的安全问题。 **（3）**华为云将安全设计阶段识别出的安全需求、攻击者视角的渗透测试用例、业界标准等作为检查项，开发配套相应的安全测试工具，在云服务发布前进行多轮安全测试，使发布的云服务满足安全要求，测试在与生产环境隔离的测试环境中进行，并避免将生产数据用于测试，如需使用生产数据进行测试，必须经过脱敏，使用完成后需要进行数据清理。

7.5 网络保安风险评估、网络攻击模拟和事故应变

原文编号	控制域	具体控制要求	华为云的应答
F1-F3	网络保安风险评估、网络攻击模拟和事故应变	F1. 进行真实网络攻击情境的模拟及最新网络攻击趋势，以确认网络防御机制是否有效。 F2. 由独立于系统开发及维护职能部门的合资格专业人士就面向互联网的系统和内部系统以及相关科技基础设施、人员和程序进行定期独立评估。 F3. 一旦发生重大安全事故（包括系统延误和失灵），即安排独立的职能部门或外部专业人士进行事后分析检讨。	客户应建立网络安全管理机制，实施网络安全评估、网络攻击模拟演练以及安全事件响应措施。为配合客户满足监管要求: **（1）**华为云定期会开展内部网络安全实战演练（如红蓝对抗）和第三方渗透测试和安全评估，监控、排查并解决安全威胁，保障云服务的安全性。 **（2）**华为产品安全事件响应团队（PSIRT – Product Security Incident Response Team）已经建立成熟的漏洞响应机制，针对云的自运营的特点，通过持续优化安全漏洞的管理流程和技术手段，以保证基础设施、平台、应用和云服务中的自研和第三方漏洞尽快修复，降低对租户业务造成影响的风险。同时，华为PSIRT和华为云安全运维团队已经建立了漏洞感知、处置和对外披露的机制。华为云依托其建立的漏洞管理体系进行漏洞管理，使基础设施、平台、应用各层系统和各项云服务以及运维工具等的自研漏洞和第三方漏洞都在SLA时间内完成响应和修复，降低并最终避免漏洞被恶意利用而导致影响租户业务的风险。

7.6 数据备份及应变计划

原文编号	控制域	具体控制要求	华为云的应答
G1-G4	数据备份及应变计划	G1. 将所有包含机密和敏感数据的备份媒体加密，并在适当情况下为有关媒体提供实体保护（例如使用上锁的盒子作保存及运输之用），以确保有关媒体得以妥为保存及运送。 G2. 定期进行数据备份的复原测试，确保能有效复原数据。 G3. 建立灾难复原/后备数据中心或作出其他替代安排，以便在主数据中心运作中断时继续向客户提供互联网交易服务，从而将该等服务所受到的干扰减至最低。 G4. 至少每年进行一次灾难复原演习，并在适当情况下更新灾难复原计划。	客户应建立备份管理机制，对机密和敏感数据进行备份，并妥善保管备份存储介质，定期进行备份恢复测试。另外，还应制定灾难恢复计划，并定期进行测试和更新。为配合客户满足监管要求： **（1）**华为云提供了多粒度的数据备份归档服务，满足客户不同场景下的需求。客户可以使用**对象存储服务（OBS）**的版本控制、**云硬盘备份（VBS）**、**云服务器备份（CSBS）**等功能，将云上的文档、硬盘、服务器进行备份，也可以通过华为云备份归档解决方案，将客户云下数据备份归档到华为云，保证在灾难发生时数据不丢失。为了提高数据灾难发生时的应急响应能力，客户可以定期依据计划进行恢复演练。华为云备份归档解决方案支持客户使用备份数据在云上即时部署的系统中恢复数据，完成后即可释放资源，极大节省了恢复演练成本。 **（2）**客户可依赖华为云数据中心集群的多地域（Region）和多可用区（AZ）架构实现其业务系统的容灾和备份，数据中心按规则部署在全球各地，客户可通过两地互为灾备中心，如一地出现故障，系统在遵循相关政策前提下自动将客户应用和数据转离受影响区域，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，客户的应用在数据中心实现N+1 部署，即便在一个数据中心故障的情况下，也可以将流量负载均衡到其他中心。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和灾难恢复计划，并定期对其进行测试。以保证应急预案符合当前的组织环境和IT环境。如果需要华为云协助执行客户的灾难恢复演练，华为会积极配合。

7.7 供货商管理 – 建立业务关系及持续审核

原文编号	控制域	具体控制要求	华为云的应答
H1-H3	供货商管理 – 建立业务关系及持续审核	H1. 在建立业务关系前评估其网络保安的抵御能力。 H2. 将以下（除其他事项外）网络保安要求列入与供货商（及／或集团内实体）订立的服务协议内： -遵循公司的网络保安政策； -上报保安事故； -在合约终止或认为有需要时，删除／销毁储存在供货商系统内的数据及备份；及 -合理的补偿保证或法律责任条文。 H3. 定期对供货商进行网络保安风险评估及现场审核，或检视供货商的审计师报告，以及要求供货商在识别到重大缺失时采取补救行动。	客户应在建立业务关系前评估供应商的网络安全能力，并将网络安全要求纳入与供应商签订的服务协议。作为云服务提供商： **（1）**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ITUE.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助力华为云安全。 **（2）**华为云提供了线上的**《华为云用户协议》**以及**《华为云服务等级协议》**，其中规定了所提供服务内容和服务水平，以及华为云的职责。同时，华为云也制定了线下合同模板，可根据不同客户的需求进行定制化。客户对华为云的审计和监督权益会根据实际情况在与客户签订的协议中进行承诺。 **（3）**华为云遵循ISO27001、ISO20000、ISO22301等国际标准建立信息安全管理体系、IT服务管理体系以及业务连续性管理体系，并在日常运营中将体系的要求落地。同时，华为云每年定期开展风险评估、管理评审等活动，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。华为云已通过ISO27001、ISO27017、ISO27018、SOC、CSA STAR等多项国际安全与隐私保护认证。华为云每年定期接受专业第三方审计机构的审核，并提供专人协助，积极响应及配合客户方发起的审计活动。

7.8 提高内部系统用户的网络保安意识

原文编号	控制域	具体控制要求	华为云的应答
I1-I2	提高内部系统用户的网络保安意识	I1. 向内部系统用户提供有系统的网络保安意识培训，包括为新入职员工开办常设课程、复修课程及按需要（例如在察觉到突如其来的网络保安威胁时）提供特殊课程，以解释与网络保安相关的公司政策和程序，以及就如何实施有关政策和程序向员工提供实用指引。 I2. 定期评估员工对公司的信息科技风险及网络保安政策的了解及遵守有关政策的情况，当中包括简短测试、提示信息（例如不要开启任何可疑邮件内的链接及附件，以免受到勒索软件的攻击）及模拟伪冒诈骗攻击。	客户应建立网络安全培训机制，定期对内部员工进行网络安全意识培训、宣传和测试。作为云服务提供商，为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，华为对全体员工从意识教育普及、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。参考业界优秀实践，华为建立了完备的网络安全培训体系。在员工入职、在岗、晋升等环节纳入多种形式的安全技能培训，提升员工安全技能，提升员工能力，向客户交付安全的产品、解决方案与服务。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。更多关于内容请参见**《华为云安全白皮书》**4.4人力资源管理。

8 结语

本文描述了华为云为客户提供的云服务如何遵从中国香港证券及期货行业监管要求，并表明华为云遵守中国香港证券及期货事务监察委员会（SFC）发布的重点监管要求，有助于客户详细了解华为云对于中国香港证券及期货行业监管要求方面的遵从性，让客户安全、放心地通过华为云服务存储、处理客户内容数据。同时，本文也在一定程度上指导客户如何在华为云上设计、构建和部署遵从中国香港证券及期货行业监管要求的安全的云环境，帮助客户更好地与华为云共同承担起相应的安全责任。

本白皮书仅供一般性参考，不具备任何法律效力或构成任何形式的法律建议，客户应酌情评估自身使用云服务的情况，并负责确保在使用华为云时对相关中国香港证券及期货行业监管要求的遵从性。

9 版本历史

日期	版本	描述
2022年4月	1.1	例行刷新
2020年9月	1.0	首次发布