瑞士金融行业监管要求遵从性指南

文档版本 1.0

发布日期 2023-06-13

华为云

HUAWEI

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。

Sparkoo Technologies Ireland Co., Ltd.

地址： 2nd Floor,
Mespil Court,
Mespil Road,
Ballsbridge, Dublin 4, Dublin,
D04 E516 , Ireland

网址： https://www.huaweicloud.com/eu/（具体请参见欧洲站华为云官网）

目 录

1 概述

1.1 背景与发布目的

随着技术的发展，对云计算技术及服务的使用已经成为瑞士金融机构的常态。云计算为金融机构的发展带来巨大的便利的同时，也为金融机构创造了更为复杂的业务运营环境。为规范金融行业对于信息科技的运用，瑞士金融市场监管局、瑞士银行家协会针对瑞士金融机构的网络安全、信息技术风险管理等方面发布了一系列监管规定。

华为云作为云服务供应商，致力于协助金融客户满足这些监管要求，持续为金融客户提供遵从金融行业标准要求的云服务及业务运行环境。本文将针对瑞士融机构在使用云服务时通常需遵循的监管要求，详细阐述华为云将如何协助其满足监管要求。

1.2 适用的金融监管要求简介

瑞士金融市场监管局（Financial Market Supervisory Authority，以下简称“FINMA”）是瑞士金融行业的监管机构，负责确保瑞士金融市场的有效运转；瑞士银行家协会（Swiss Bankers Association，以下简称“SBA”）是全球最大的银行业行业公会，其会员涵盖了瑞士的银行、审计机构和券商等，在瑞士以及国际金融界都有着重大影响。

- 《第2018/3号通告 外包》（Circular 2018/3 Outsourcing）：FINMA于2017年9月21日发布了该通告，其规定了银行、券商和保险公司在开展重要功能外包活动时必须遵守的要求。
- 《第2023/1号通告 操作风险和弹性--银行》（Circular 2023/1 Operational risks and resilience--banks）：FINMA于2022年12月7日发布了该通告，对《第2008/21号通告 操作风险--银行》进行了全面修订，完善了与操作风险管理相关的监管实践，在其基础上新增操作弹性的原则。监管领域包括总体操作风险管理、ICT风险管理、网络风险管理、关键风险管理、业务连续性管理、跨境事务风险管理以及保证操作弹性等。
- 《云指南》（Cloud Guidelines）：SBA于2020年6月1日发布了该指南，确定了与通过云技术提供银行和金融服务相关的四个关键领域，包括治理、数据和数据安全、权限和程序、对所使用的云服务和手段的审计。指南中就如何管理这些领域提出了建议。这些建议不具有法律约束力。银行可在考虑到其规模和业务模式的复杂性的情况下，将该指南作为最佳实践加以应用。

- 《第05/2020号指南》（Guidance 05/2020）：FINMA于2020年5月7日发布了该指南，对所有FINMA所监管的机构提出了在发生具有重大影响的网络攻击事件时向监管机构报告的要求，并且明确了履行报告义务的细节规定。

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。

- **客户**

  指与华为云达成商业关系的注册用户。

- **外包**

  指金融机构授权服务提供商独立地、持续地履行对其业务活动有重要意义的全部或部分职能。

- **重要职能**

  指对遵守金融市场立法的目的和规定有重大影响的职能。

- **关键数据**

  指基于金融机构的规模、复杂性、结构、风险状况和业务模式，具有重要意义的，需要加强对其实施的安全措施的数据。这些数据对于金融机构提供服务或监管至关重要。

- **关键流程**

  指那些发生重大破坏时，将会危及重要职能的提供的流程。

- **ICT**

  指 IT 和通信系统的物理和逻辑（电子）架构、各个硬件和软件资产、网络、数据和操作环境。

- **客户识别数据**

  指那些能够反映个人数据，并识别所涉及客户的客户数据。

- **受保护信息**

  指客户识别数据、个人数据以及金融机构所指定的需要保密处理的其他信息和数据。

- **重要分包商**

  指履行重要职能的分包商，以及金融机构视为重要的分包商。

2 华为云安全合规

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
ISO20000-1:2011	ISO20000 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。
ISO27001:2013	ISO27001 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。
ISO27017:2015	ISO27017 是针对云计算信息安全的国际认证。ISO27017 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。
ISO22301:2012	ISO22301 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。
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(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

认证	描述
CCEAL3+	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。
ISO27018:2014	ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 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。
ISO29151:2017	ISO29151 是国际个人身份信息保护实践指南。ISO29151 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。
ISO27701:2019	ISO27701 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。
BS10012:2017	BS10012 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
中国网络安全等级保护	网络安全等级保护是中华人民共和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，目前已成为中国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。

认证	描述
新加坡 MTCS Level3 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 Level3 等级认证。
中国可信云金牌运维专项评估	金牌运维评估是面向已通过中国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，符合中国权威云服务运营和维护保障要求的认证标准。
中国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。
中国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》等相关中国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。
中国可信云评估	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。
中国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。

目前，爱尔兰 Sparkoo 也已获得众多国际和行业安全合规资质认证，主要包括：

认证	描述
ISO27001:2013	ISO27001 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。
ISO27017:2015	ISO27017 是针对云计算信息安全的国际认证。ISO27017 的通过，表明爱尔兰 Sparkoo 在信息安全管理能力达到了国际公认的最佳实践。
ISO27018:2014	ISO27018 是专注于云中个人数据保护的国际行为准则。ISO27018 的通过，表明爱尔兰 Sparkoo 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。
ISO29151:2017	ISO29151 是国际个人身份信息保护实践指南。ISO29151 的通过，表明爱尔兰 Sparkoo 实施国际认可的个人数据处理的全生命周期的管理措施。
BS10012:2017	BS10012 是 BSI 发布的个人信息数据管理体系标准，

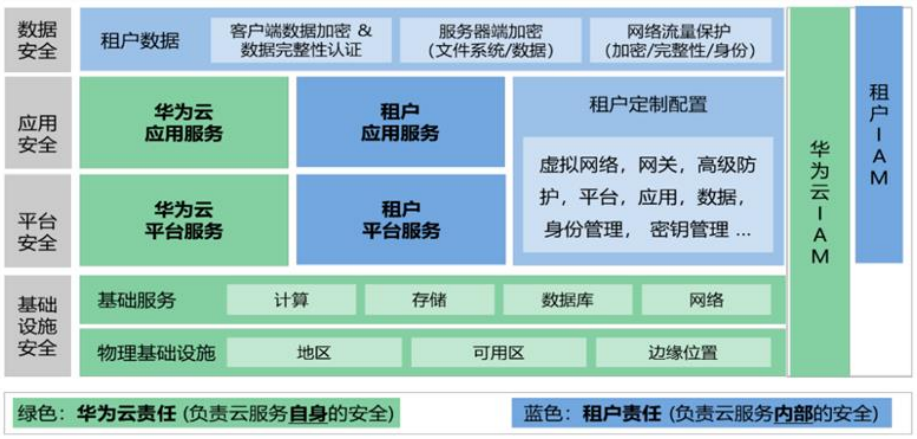
	BS10012 认证的通过表明爱尔兰 Sparkoo 在个人数据保护上拥有完整的体系以保证个人数据安全。
ISO27701:2019	ISO27701 规定了建立、实施、维护和持续改进隐私相关所特定的管理体系的要求。爱尔兰 Sparkoo 通过 ISO27701 表明了其在个人数据保护具有健全的体制。
ISO20000-1:2011	ISO20000 是针对信息技术服务管理领域的国际标准，提供设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的模型以保证服务供应商可提供有效的 IT 服务来满足客户和业务的需求。
ISO22301:2012	ISO22301 是国际公认的业务连续性管理体系标准，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。
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。
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。
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。
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。

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

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瑞士《第 2018/3 号通告 外包》

FINMA 于 2017 年 9 月 21 日发布了《第 2018/3 号通告 外包》。该通告规定了银行、券商和保险公司在开展重要功能外包活动时必须遵守的要求。

金融机构在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

5.1 选择、指导和监督服务提供商

编号	具体控制要求	客户关注点	华为云的内部实践
第 17 条	选择服务提供商时，金融机构应适当考虑并检查其专业能力与财务和人力资源情况。	客户应在尽职调查中考虑服务提供商的专业能力、人力资源以及财务情况等。	华为云会安排专人积极配合客户发起的审计要求和尽职调查。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，并且每年会接受第三方的审计。 ●专业能力：华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立完善的信息安全管理体系、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。 ●人员管理：华为云严格执行长期以来行之有效的人事和人员管理机制。华为云全体员工、合作伙伴及外部顾问都必须遵从公司相关安全政策，接受安全培训，使安全理念融入整个组织中。华为云对积极执行网络安全保障政策的员工给予奖励，对违反的员工给予处罚，违反相关法律法规的员工，还将依法承担法律责任。 ●财务状况：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。
第 18 条	在决定外包和选择服务提供商时，金融机构应考虑更换服务提供商的可能性及其可能产生的后果。服务提供商应保证能够长期提供服务。	客户应在尽职调查中考虑服务提供商的专业能力，以保证其能够为向客户长期提供服务。	华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立完善的信息安全管理体系、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。
第 18.1 条	金融机构应为将外包职能内包或将其有序地转移到另一服务提供商而做好准备。	客户应在云外包协议中明确定义退出策略条款，包括支持数据迁移义务。 在服务协议终止时，客户可通过华为云提供的云数据迁移服务（Cloud Data Migration，简称 CDM）支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。

		之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。	
第 19 条	金融机构和服务提供商的职责应在合同中达成一致并明确。	客户应在云外包协议中明确其与服务提供商各自的职责。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。例如，华为云负有一定的安全义务，应采取适当措施保护客户数据的安全，并且在非必要的情况下，不得访问客户的数据。同时，客户也负有一定的安全义务，应对由于其使用账号和服务的方式等原因所导致的安全漏洞负责。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。
第 20 条	外包职能应被纳入金融机构的内部控制体系。与外包有关的重大风险应被系统地识别、监测、量化和控制。金融机构内部应指定部门负责监测和控制服务提供商。金融机构应持续监测和评估服务提供商的服务，以便及时采取必要措施。	客户应对服务提供商进行持续的监督，从而识别和处置与外包相关的重大风险。	客户对华为云的审计和监督权益会根据实际情况在与金融机构签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。
第 21 条	金融机构应确保与服务提供商的外包协议赋予其发布必要指示和控制的权利。	客户应在云外包协议中明确其拥有向服务提供商发布必要指示与控制的权利。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。 华为云专业的服务工程师

			团队提供 7*24 小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。

5.2 安全性

编号	具体控制要求	客户关注点	华为云的内部实践
第 24 条	若与安全有关的职能被外包（特别是在 IT 方面），金融机构和服务提供商应在合同中约定安全要求。金融机构应监督这些要求的遵守情况。	客户应在云外包协议中明确安全要求，同时对服务提供商的遵守情况进行监督。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。例如，在外包协议中明确约定华为云应当遵守的安全要求。 客户对华为云的审计和监督权益会根据实际情况在与金融机构签订的协议中进行承诺。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。
第 25 条	金融机构和服务提供商应制定安全框架，以确保在紧急情况下仍能继续执行外包职能。对此，金融机构应采取与其执行外包职能时相同程度的谨慎与关注。	客户应制定业务连续性计划，定期测试和更新，同时与服务提供商相协调。	华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。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。 如果客户在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。

5.3 审计和监督

编号	具体控制要求	客户关注点	华为云的内部实践
第 26 条	金融机构、FINMA 以及其指定的审计机构应能够核实服务提供商是否遵守监管法规。外包协议应规定它们拥有在任何时候不受限制地检查和审计所有与外包职能有关信息的权利。	客户应确保外包书面协议中规定相应的访问权、审计权和监督权。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。 目前，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，并且每年会接受第三方的审计。
第 29 条	若服务提供商不受 FINMA 监督，则外包协议中应明确服务提供商负有向 FINMA 提供与外包职能有关信息和文件的义务。若审计工作被委托给服务提供商的审计人员，则审计报告应按要求提供给 FINMA 以及金融机构的内审人员和指定的审计机构。	客户应确保外包书面协议中规定相应的访问权、审计权和监督权。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。华为云会遵从与客

			户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。

5.4 外包到国外

编号	具体控制要求	客户关注点	华为云的内部实践
第 30 条	若金融机构能够确保其、其 FINMA 以及其指定的审计机构能够主张并执行检查和审计信息的权利，则允许外包至其他国家。	客户应确保外包书面协议规定相应的访问权、审计权和监督权。	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。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。

5.5 协议

编号	具体控制要求	客户关注点	华为云的内部实践
第 32 条	外包应以书面协议或其他格式的协议为基础。这些协议应能够以文本形式证明。外包协议内容应包括缔约方名称与职能。	客户应与服务提供商签订书面外包协议，并在其中明确缔约各方的名称与职能。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。
第 33 条	外包协议内容应包括金融机构在服务提供商使用或更换重要职能分包商时应被事先告知，并且对此有权有序终止外包。分包商也应遵守服务提供商为遵守本通知所履行的义务。	客户应确保外包书面协议规定以下内容： a. 使用或更换分包商时应事先告知客户； b. 客户有权因使用或更换分包商而终止外包； c. 分包商应遵守服务提供商为符合本通知所履行的义务。	

第 34 条	外包协议内容应包括金融机构发布必要指示的权利、金融机构与服务提供商约定的安全要求、服务提供商配合监管活动的义务以及金融机构等开展审计的权利。	客户应确保外包书面协议规定以下内容： a. 向服务提供商发布必要指示与控制的权利； b. 合同各方约定的安全要求； c. 服务提供商配合监管的义务； d. 相关方的审计权利。	

6 华为云如何遵从及协助客户满足瑞士《第 2023/1 号通告 操作风险和弹性--银行》

FINMA 于 2022 年 12 月 7 日发布了《第 2023/1 号通告 操作风险和弹性--银行》。该通告对《第 2008/21 号通告 操作风险--银行》进行了全面修订，完善了与操作风险管理相关的监管实践，在其基础上新增操作弹性的原则。监管领域包括总体操作风险管理、ICT 风险管理、网络风险管理、关键风险管理、业务连续性管理、跨境事务风险管理以及保证操作弹性等。

金融机构在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

6.1 ICT风险管理

编号	具体控制要求	客户关注点	华为云的内部实践
第 51 条	金融机构应确保开发或测试环境与 ICT 生产环境分离。	客户应建立和实施环境隔离措施，确保生产环境与非生产环境的隔离。	华为云建立了正式的环境隔离机制，对开发环境、测试环境及生产环境实现严格的逻辑隔离，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。禁止未经授权打通测试环境和生产环境的网络链接，避免因测试环境被入侵而导致生产环境安全风险。同时，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，确保开发和运维人员职责分离。
第 56 条	金融机构应确保能够在 ICT 运行发生严重中断时，顺利过渡实施业务连续性计划和灾难恢	客户应制定业务连续性计划与备份和恢复计划，并定期	华为云遵循 ISO22301 业务连续性管理国际标准，建立了一套完善的业务连

	复计划。此外，金融机构还应实施适当的备份和恢复流程，定期测试和验证。	进行测试、验证和更新。 客户可以通过云备份（Cloud Backup and Recovery，简称 CBR）服务支持客户对数据进行备份，保证在灾难发生时数据不丢失。	续性管理体系。在该体系框架下，定期进行业务影响分析和风险评估。为支撑云服务持续运行的关键业务制定了完善的恢复策略。恢复策略涵盖备用场地、设备、人员、信息系统、第三方等各个方面，并定期测试备份和恢复程序。
第 57 条	金融机构应制定和实施适当流程与控制措施，确保通过风险导向的方式处理运行寿命即将结束或计划停用的 ICT。	客户应采取适当措施妥善处置计划停用的 ICT 资产。	当客户主动进行数据删除操作或因服务期满需要对数据进行删除时，华为云会严格遵循适用的法律法规，以及与客户之间的协议约定，按照数据销毁标准清除客户的数据。为了避免重要数据销毁后不可恢复，或因误操作丢失，建议客户在销毁数据之前慎重考虑，对拟销毁的数据做好备份或迁离。
第 58 条	金融机构应制定和实施适当的流程与控制措施，以处理包括因依赖外部服务提供商和集团内外包业务而产生的事件在内的重大 ICT 事件。	客户建立并实施事件和问题管理流程，以监测和记录运营和安全事件，并在发生中断时能够及时恢复关键业务职能和流程。 云监控服务（Cloud Eye Service，简称 CES）为客户提供了一个针对弹性云服务器、带宽等资源的立体化监控平台。可协助客户快速获取云资源的告警，采取相应的应对措施。	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保

			障客户云服务的持续运行。 华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。
第 59 条	金融机构处理重大 ICT 事件应与业务连续性计划和灾难恢复计划相协调。	客户应制定处理重大安全事件的制度、流程与控制措施，并确保其与业务连续性计划以及灾难恢复计划相协调。	华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。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。 如果客户在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。
第 60 条	若金融机构认为 ICT 事件对其关键流程造成重大中断，同时其对监管活动具有重大意义，则应立即向 FINMA 报告。	客户建立并实施事件和问题管理流程，以及时向监管机构报告重大安全事件。 云监控服务（Cloud Eye Service，简称 CES）为客户提供了一个针对弹性云服务器、带宽等资源的立体化监控平台。可协助客户快速获取云资源的告警，采取相应的应对措施。	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。

			华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保障客户云服务的持续运行。 华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。

6.2 网络风险管理

编号	具体控制要求	客户关注点	华为云的内部实践
第 62 条	金融机构应明确任务、权限和责任，至少应包括以下方面： a. 从网络攻击中识别特定机构的威胁态势，评估利用漏洞可能对已清点的 ICT 资产与电子关键数据造成的影响； b. 通过实施适当保护措施，特别是针对保密性、完整性和可用性，保护已清点 ICT 资产和电子关键数据面授网络攻击； c. 针对已清点的 ICT 资产和电子关键数据进行系统与持续监控，及时记录和发现网络攻击；	客户应采取适当措施，确保 ICT 资产的安全。	华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。 华为云在用户协议中明确

	d. 通过制定和实施适当流程，快速采取控制与补救措施，响应已经查明的漏洞与网络攻击； e. 实施适当措施，确保在网络攻击后业务运作能够迅速恢复正常。		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，或者为遵守法律法规或政府机关的约束性命令，并严格遵守适用与客户的所有有关数据保护的法律规定。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。此外，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。 为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，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。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。同时，华为云也根据内部业务连续性管理体系的要求，制定了危机

			沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。 华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。并根据事件的实时状态进行事件升级和通报。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，将事件通知客户。通知内容包括事件的描述、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。 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。同时，华为云会积极实施云产品和云平台的安全质量保证工作，每年会开展内部和第三方渗透测试和安全评估，以保证华为云云环境的安全性。 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。此外，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，预案中详细规定了应急响应的组织、程序与操作规范等，并定期进行测试，每年会对重大的安全风险场景进行应急演练，以确保在发生此类安全事件时，快速削减可能产生的安全

			风险，确保云服务持续运行，保障客户的业务和数据安全。
第 68 条	金融机构应在 24 小时内对网络攻击开展初步评估，完成初步评估后通知 FINMA。金融机构应在 72 小时内向 FINMA 提交内容符合要求的详细报告。金融机构应在完成针对网络攻击的处理后，向 FINMA 提交与网络攻击严重程度相符的关于根本原因分析。	客户应在规定时间内完成对网络攻击的评估并向监管机构提交包含相应内容的报告以及根本原因分析。	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，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。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。
第 69 条	金融机构应定期安排专业人员针对所有已清点的 ICT 资产开展漏洞评估与渗透测试。	客户应对 ICT 资产进行测试，识别潜在的安全弱点和违规事件。如代码审查、渗透测试、漏洞扫描等。	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。同时，华为云会积极实施云产品和云平台的安全质量保证工作，每年会开展内部和第三方渗透测试和安全评估，以保证华为云云环境的安全性。
第 70 条	金融机构应开展网络安全演习，并以适当形式记录和报告网络安全演习的结果。	客户应定期开展网络安全演练，并记录与报告演练结果。	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。

6.3 关键数据风险管理

编号	具体控制要求	客户关注点	华为云的内部实践
第 76 条	金融机构应充分保护关键数据，以防止未经授权人员访问和使用。	客户应实施安全措施，以保护数据不被未经授权的访问。 为防止内容数据被异常下载，针对不同的产品和服务，客户可使用不同的方式进行审计，检测异常活动。如对于对象存储、文件存储等服务，客户可以使用云审计服务（Cloud Trace Service，简称 CTS）来记录用户对数据的操作。对于关系型数据库服务，客户可以使用数据库安全服务来进行数据库列级的管理和访问活动记录。	华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。 华为云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，或者为遵守法律法规或政府机关的约束性命令，并严格遵守适用与客户的所有有关数据保护的法律规定。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。此外，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。
第 77 条	金融机构应保护存储或处理关键数据的 ICT 资产，并系统性规范和持续监测针对关键数据的访问。	客户应通过日志监控异常活动，并定期审查和分析。 华为云的云审计服务（Cloud Trace	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

		Service，简称 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。 华为云提供的云日志服务（Log Tank Service，简称 LTS）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。	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。
第 78 条	对关键数据的访问与处理功能的使用应仅限于需借此执行任务的人员。金融机构应建立授权系统，并保护与定期审查对该系统的访问，同时定期审查该系统中的授权情况。	客户应确保对关键数据和系统的访问遵循“最小权限原则”。 客户可使用华为云的统一身份认证服务（Identity and Access Management，简称 IAM）对使用云资源的用户账号进行管理。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	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。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。

		入。同时，客户应建立用户访问管理机制，基于最小权限原则进行访问系统权限限制和监督。	
第 79 条	若关键数据存储在瑞士境外，或其可从瑞士境外被访问，则金融机构应实施适当措施保护关键数据，监测并减轻相关风险。	客户应采取适当的安全措施保护关键数据的安全，持续监测并减轻相关风险。 客户可使用华为云提供的多种隐私保护技术及服务，包括统一身份认证服务（Identity and Access Management，简称IAM）、数据加密服务（Data Encryption Workshop，简称DEW）、云日志服务（Log Tank Service，简称LTS）和云审计服务（Cloud Trace Service，简称CTS）等，为客户提供访问控制和身份认证、数据加密、日志和审计等功能，帮助客户根据业务需求进行个人数据保护。	华为云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，或者为遵守法律法规或政府机关的约束性命令，并严格遵守适用与客户的所有有关数据保护的法律规定。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。 华为云严格遵守所有适用的与客户有关数据安全和隐私保护的法律规定的要求。在数据跨境传输方面，华为云为客户提供签署和查询隐私通知的接口，将数据可能转移至欧境外告知其数据主体。客户可根据需要选择存储内容数据的服务器区域。未经客户同意，华为云不会将客户的内容数据从所选服务器区域迁出。 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。 华为云已通过 ISO 27001、ISO 27017、ISO 27018、SOC、CSA STAR 等多项国际安全与隐私保护认证，华为云目前获得了国际上多项权威

			的安全与隐私保护认证，第三方测评公司也会定期对华为云展开保密性、安全充分性和合规性的审核并出具第三方审计报告。关于第三方审计报告的获取的要求，可以根据实际情况在客户签订的协议中约定。为配合客户满足合规要求，华为云参照各类法规要求、监管要求、国际或行业标准建立了一套完善的信息安全和隐私保护管理体系，并持续改进。同时，华为云定期会开展内部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。
第 80 条	金融机构应谨慎选择有权访问与更改关键数据的内外部人员，并通过实施适当措施对此类人员进行监督，同时为其处理关键数据提供定期培训。金融机构还应保存与定期更新拥有特许访问权限的人员清单。	客户应制定并实施安全意识培训计划。并对关键岗位实施专门的人员管理计划，并定期对其进行 IT 安全行为的培训。	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，华为云从意识教育普及、宣传活动开展、员工商业行为准则及承诺书签署三个方面开展安全意识教育，有专门的信息安全意识培训计划，并每年至少执行一次针对全员的安全意识培训，意识教育的形式包括但不限于现场演讲、视频网课等。 同时，为了有序管理，降低人员管理风险对业务连续性和安全的潜在影响，华为云针对运维工程师等关键岗位实施了专门的人员管理计划，包括入职安全审查、在职安全培训与赋能、入职资格管理、离职安全审查。
第 81 条	金融机构应立即向 FINMA 报告严重损害关键数据机密性、完整性和可用性的事件。	客户建立并实施事件和问题管理流程，以及时向监管机构报告重大安全事件。	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影

			响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。 华为云部署了全网告警系统，对网络设备资源使用率进行持续监控，监控范围覆盖所有网络设备。在资源使用率达到预设阈值时，告警系统将发出警告，运维人员将及时采取解决措施，最大限度地保障客户云服务的持续运行。 华为云拥有 7*24 的专业安全事件响应团队负责实时监控告警。根据事件定级标准以及响应时限和解决时限等要求，能够快速发现、快速定界、快速隔离与快速恢复的事件。并根据事件的实时状态进行事件升级和通报。且华为云会定期对事件进行统计和趋势分析，针对类似事件，问题处理小组会找到根本原因，并制定解决方案从根源上杜绝该类事件的发生。
第 82 条	在选择能够处理或查看关键数据的服务提供商时，金融机构应开展详细的尽职调查，了解服务提供商处理关键数据的标准，并监督和定期检查服务提供商的实施情况。	客户应对能够处理或访问关键数据的服务提供商开展尽职调查，以了解其处理关键数据的标准，同时还应监督与定期检查实施情况。	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。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。

6.4 业务连续性管理

编号	具体控制要求	客户关注点	华为云的内部实践
第 85 条	金融机构应确定关键流程的恢复时间目标与恢复点目标，与服务提供商相协调，同时通过合同等方式规范服务提供商的遵守情况。	客户应进行业务影响分析，识别关键业务，确定关键流程的 RTO 和 RPO。同时，客户应在外包协议中明确相关内容，规范服务提供商的遵守情况。	华为云遵循 ISO22301 业务连续性管理国际标准的要求，建立了一套完善的业务连续性管理体系。在该体系框架的要求下，华为云定期开展业务影响分析、识别关键业务、确定关键业务的恢复目标及最小恢复水平。在识别关键业务的过程中，将业务中断对客户的影响程度作为判断关键业务的一个重要标准。 如果客户在运行其组织内部的业务连续性计划的过程中需要华为云的参与，华为云会积极配合。
第 87 条	金融机构应准备和记录业务影响分析与业务连续性计划，每年对其进行审查和更新，或者在业务运营情况发生重大变化时进行临时性审查和更新。	客户应制定业务连续性计划，并定期对其进行测试和更新，以维持恢复策略的有效性。	华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。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、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。

第 90 条	金融机构应明确危机发生时的内外部沟通策略。	客户应制定和实施危机沟通策略。	华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通。华为云专业的服务工程师团队提供 7*24 小时的服务支持，客户可以通过工单、智能客服、自助服务、热线电话等联络到华为云的支持团队。同时，华为云也根据内部业务连续性管理体系的要求，制定了危机沟通策略，定义了突发事件下需要沟通的对象、沟通的内容、沟通的工具等。
第 91 条	金融机构应制定计划，通过不同测试手段，定期评估业务连续性计划以及灾难恢复计划的运行情况。	客户应制定业务连续性计划和灾难恢复计划，并定期对其进行测试，以维持恢复策略的有效性。	华为云制定了灾难恢复计划，并定期对其进行测试。例如，将一个地理位置或区域的云平台基础架构和云服务处于离线状态，模拟一个灾难，然后按照灾难恢复计划进行系统处理和转移，以验证故障位置的业务及营运功能，测试结果将被注释并记录归档，用以持续改进该计划。 华为云拥有丰富的业务连续性管理和灾难恢复策略和流程。业务连续性计划每年由业务连续性管理团队制定和审查，并根据审查结果更新计划。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、最大可容忍停机时间、恢复时间目标、最低服务级别和恢复服务所需的时间。报告中识别并记录了可能导致华为云业务和资源中断的威胁，并针对华为云产品的不同服务中断场景设计了相应的策略。业务影响分析和风险评估的结果记录在风险评估报告中。华为云根据计划，至少每年对所有范围内产

			品进行业务连续性演练测试。记录和审查业务连续性演练测试的结果。
第 96 条	针对负责处理危机事件的员工，金融机构应自其加入时起，定期开展与业务连续性管理活动所涉及的任务、权限和责任有关的培训。	客户应定期对相关员工开展业务连续性方面的培训。	华为云制定了符合自身业务特色的业务连续性管理体系，为客户持续有效提供服务，保证客户业务的开展。华为云每年会在组织内进行业务连续性的宣传和培训，针对危机管理岗位的员工开展专门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 华为云如何遵从及协助客户满足瑞士《云指南》

SBA 于 2020 年 6 月 1 日发布了《云指南》。该指南确定了与通过云技术提供银行和金融服务相关的四个关键领域，包括治理、数据和数据安全、权限和程序、对所使用的云服务和手段的审计。指南中就如何管理这些领域提出了建议。这些建议不具有法律约束力。银行可在考虑到其规模和业务模式的复杂性的情况下，将该指南作为最佳实践加以应用。

金融机构在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

7.1 责任和作用

编号	具体控制要求	客户关注点	华为云的内部实践
第 10 条	在明确金融机构与服务提供商以及分包商等相关方的角色时，服务与交付模式应被考虑。服务提供商应在必要与适当时向金融机构提供相关信息。	客户应确保在外包协议中明确其与服务提供商以及相关各方的角色。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。例如，华为云负有一定的安全义务，应采取适当措施保护客户数据的安全，并且在非必要的情况下，不得访问客户的数据。同时，客户也负有一定的安全义务，应对由于其使用账号和服务的方式等原因所导致的安全漏洞负责。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。
第 12 条	金融机构与服务提供商的合同中应明确各相关方的权利和义务以及与其执行有关的规定。	客户应在外包协议中明确分配和规定各相关方的职责。	

7.2 选择和变更服务提供商与重要分包商

编号	具体控制要求	客户关注点	华为云的内部实践
第 14 条	金融机构在选择服务提供商时，应考虑履行合同的能力、财务情况等因素。服务提供商的重要分包商也应被纳入评估范围。服务提供商应协助金融机构收集相关信息。	客户应在尽职调查中考虑服务提供商的专业能力、财务情况以及供应商管理等。	华为云会安排专人积极配合客户发起的审计要求和尽职调查。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，并且每年会接受第三方的审计。 ●专业能力：华为云遵循 ISO27001、ISO20000、ISO22301 等国际标准建立完善的信息安全管理体系、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。 ●财务状况：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。 ●供应商管理：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。此外，华为云会对供应商进行定期的稽核，对有风险的供应商会到现场进行审核。此外，华为云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。

第 16 条	在选择服务提供商时，除业绩相关标准外，金融机构应考虑服务提供商的合规情况与运营模式。此外，在选择服务提供商及分包商处理金融机构的客户识别数据或其他个人数据时，金融机构应考虑到服务提供商的对数据机密性与安全性的保护。	客户应在尽职调查中考虑服务提供商的业绩情况、合规情况以及信息安全管理等。	华为云会安排专人积极配合客户发起的审计要求和尽职调查。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，并且每年会接受第三方的审计。此外，华为云将积极配合金融机构满足监管机构相关的要求。 ●业绩情况：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。 ●合规情况：面向提供云服务的地区，华为云积极与监管机构对话，理解他们的担忧和要求，贡献华为云的知识和经验，不断巩固华为云在云技术、云服务和云安全方面与相关法律法规的契合度。同时，华为云也将法律法规的分析结果共享给租户，避免信息缺失导致的违规风险，通过合同明确双方的安全职责。华为云一方面通过跨行业、跨区域的云安全认证满足监管机构要求，另一方面通过获得重点行业、重点区域所要求的安全认证，建立并巩固华为云业务的客户信赖度，最终在法律法规制定者、管理者、租户三者间共建安全的云环境。 ●信息安全管理：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。此外，华为云重点关注员工以及外包人员的安全意识培养，制定了可落地的安全意识培训计划并定期执行。
第 17 条	变更服务提供商应事先征得金融机构的书面同意。若重组发生在同一集团内部以及相同管辖区范围内，并且对服务现状、规格以及风险无重大影响，则无须征得同意。此外，服务提供商应按照金融机构的要求对相关变更做出安排。	客户应在外包协议中规定变更服务提供商应事先征得客户同意。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。
第 18 条	服务提供商应在使用新的重要分包商前通知金融机构。金融机构有权因此终止外包，同时采取适当措施有序转移外包职能。	客户应确保外包书面协议规定以下内容： a. 使用或更换新的重要分包商时应事先告知客户； b. 客户有权因使用或更换分包商而终止外包； c. 退出策略条款，包括支持数据迁移义务。 在服务协议终止时，客户可通过华为云提供的云数据迁移服务（Cloud Data Migration，简称 CDM）支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并	

		且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。	

7.3 数据中心和运营中心

编号	具体控制要求	客户关注点	华为云的内部实践
第 20 条	服务提供商应披露金融机构部署或可部署的数据中心与运营中心的位置以及部署期间位置的变化。该披露还应包括运营、拥有或以其他方式控制数据中心和运营中心的法律实体相关信息，特别是服务提供商和重要分包商。	服务提供商应向客户披露数据中心与运营中心所在位置等相关信息。	华为云提供了线上的《数据处理附录》(具体请参见欧洲站的数据处理附录)，其中明确披露了客户可部署的数据中心所在位置（当前华为云欧洲站数据中心部署在爱尔兰，欧洲站数据中心部署位置会不时更新）等相关信息。若在客户部署期间数据中心与运营中心位置发生变化，华为云将及时更新相关信息。同时，华为云也将根据客户需求向其披露相关信息，例如与重要分包商有关的信息。
第 21 条	当涉及受保护信息时，若在合同期内需将地点变更至另一管辖区，则应遵守合同规定的变更程序，并根据特定需要，征得金融机构的事先同意。服务提供商应详细说明与地点变更有关的风险，并向金融机构提供所有相关信息，特别是关于所适用的安全措施的信息，以便其能够做出决定。	当涉及受保护信息时，客户应确保外包书面协议规定以下内容： a. 变更程序； b. 变更数据中心和运营中心的位置时，事征得客户先同意（客户视具体情况确定）。 服务提供商应向客户提供相关信息，使其充分了解变更地点的相关风险。 如果客户有数据迁移的需求，可通过	华为云以区域（Region）为单位向客户提供服务。区域即客户内容数据的存储位置，华为云绝不会在未经用户授权的情况下，跨区域移动客户的内容数据。客户在使用云服时，建议根据就近接入原则并遵从不同地域的法律法规要求选择区域，确保其内容数据存储在目标位置。 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》（具体请参见欧洲站的用户协议和云服务等级协议），其中规定了所提供服务内容和服务水平，以及华为

		华为云的云数据迁移服务（Cloud Data Migration，简称 CDM）实现。	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。 华为云作为认可机构的服务提供方，会积极配合认可机构主动发起的沟通，提供相应的材料。
第 22 条	金融机构有权无理由拒绝事先同意。金融机构有权因地点变更终止外包，同时采取适当措施有序转移外包职能。	客户应确保外包书面协议规定以下内容： a. 客户有权因数据中心和运营中心的位置变更而终止外包； b. 退出策略条款，包括支持数据迁移义务。 在服务协议终止时，客户可通过华为云提供的云数据迁移服务（Cloud Data Migration，简称 CDM）支持在多种类型数据源之间进行数据迁移，例如数据库、数据仓库、文件等，并且支持在多个环境之间进行数据迁移，满足数据上云、云中数据交换、数据回流本地数据中心等多种业务场景需求。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。

7.4 存储地点、数据流和访问概念

编号	具体控制要求	客户关注点	华为云的内部实践
第 27 条	金融机构有权了解受保护信息的存储位置，检查其可接受性，并向其客户披露该位置。	客户应有权了解服务提供商存储数据的位置，并向其客	华为云目前已陆续在全球多个国家或地区提供云服务，其基础设施部署在全

	为此，服务提供商应向金融机构提供相应信息。	户披露该位置信息。	球多个地理区域（Region）和多个可用区（AZ）。通过该部署模式，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和存储实例资源。每个可用区都是一个独立故障维护域，即各可用区在物理上是隔离的，用户可充分利用这些地理区域和可用区规划、部署和运行云上应用系统。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应用系统都能持续运行。关于更多华为云基础设施信息，参见华为云官网“全球基础设施”。华为云以区域（Region）为单位向客户提供服务。区域即客户内容数据的存储位置，华为云绝不会在未经用户授权的情况下，跨区域移动客户的内容数据。客户在使用云服务时，建议根据就近接入原则并遵从不同地域的法律法规要求选择区域，确保其内容数据存储在目标位置。对于区域服务，客户可以在购买服务初期按需选择区域，其服务部署位置及数据留存地可以通过华为云门户进行变更。
第 28 条	若服务提供商以及相关分包商之间涉及受保护信息的传输，服务提供商应事先向金融机构披露。如果需要，应在外包协议中尽可能准确地说明数据流。	在服务提供商以及相关分包商之间涉及受保护信息的传输的情况下，客户应结合自身需要，确保在外包协议中包括受保护信息的数据流的结构。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。若客户明确要求，华为云将会在与客户签署的数据处理协议中披

			露分包商以及数据流相关信息。
第 29 条	金融机构有权了解对受保护信息的访问授权情况，并以适当方式监督和记录对受保护信息的访问。	客户有权了解对受保护信息的访问授权，并记录与监督对受保护信息的访问。	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。在权限复核与调整方面，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。 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。

7.5 关于数据安全的一般技术和组织措施

编号	具体控制要求	客户关注点	华为云的内部实践
第 31 条	服务提供商应根据合同中约定实施适当的技术与组织措施，以保护其正在处理的金融机构的受保护信息。国际标准与地方标准应被参考。分包商以及分包商和服务提供商部署的工作人员应遵守这些措施。	客户应确保在外包协议中规定适当的技术与组织措施。服务提供商及其分包商的员工都应遵守相关措施。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。此外，其中还包括了华为云所实施的安

			全措施。例如，加密、访问控制、事件管理、配置管理、对华为云开展第三方安全审计等。华为云将持续更新和完善安全措施，确保客户数据的安全性。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。 华为云高度重视用户的数据信息资产，把数据保护作为华为云安全策略的核心。华为云将继续遵循数据安全生命周期管理的业界先进标准，在身份认证、权限管理、访问控制、数据隔离、数据传输、数据存储、数据删除、物理销毁等方面，采用优秀的技术、实践和流程，为用户提供有效的数据保护能力，保障用户对其数据的隐私权、所有权和控制权不受侵犯。 华为云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，或者为遵守法律法规或政府机关的约束性命令，并严格遵守适用与客户的所有有关数据安全和隐私保护的法律规定。同时，在与客户签订的合同中会明确规定违反保密条款的情况下华为云应对客户承担的责任。此外，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。 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。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。
第 32 条	服务提供商应确保其员工与分包商员工做出保密承诺，并对数据进行相应处理。此外，员工还应接受相关培训。	服务提供商与分包商员工应做出保密承诺，并对其员工开展定期培训。	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，华为云从意识教育普及、宣传活动开展、员工商业行为准则及承诺书签署三个方面开展安全意识教育，有专门的信息安全意识培训计划，并每年至少执行一次针对全员的安全意识培训，意识教育的形式包括但不限于现场演讲、视频网课等。

7.6 银行保密和安全措施

编号	具体控制要求	客户关注点	华为云的内部实践
第 33 条	金融机构应采取适当的技术与组织等方面的安全措施，维护使用云服务处理的客户识别数据的安全。金融机构需考虑实施的安全措施记载于《第 2008/21 号通告》（该通告已被《第 2023/1 号通告 操作风险和弹性--银行》全面修订）。	客户应采取适当的技术与组织等方面的安全措施，维护使用云服务处理的客户识别数据的安全。	详情可参考“6.华为云如何遵从及协助客户满足瑞士《第 2023/1 号通告 操作风险和弹性--银行》”中华为云的内部实践情况。

7.7 权限和程序

编号	具体控制要求	客户关注点	华为云的内部实践

第 57 条	针对有关当局要求移交通过云服务处理的受保护信息，服务提供商应与金融机构商定相应的响应流程，并在合同中予以明确。	客户应确保在外包协议中明确针对有关当局要求移交通过云服务处理的受保护信息的响应流程。	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》（具体请参见欧洲站的用户协议和云服务等级协议），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。
第 58 条	服务提供商应在与金融机构的合同中明确，在外国诉讼的情况下，服务提供商、其分包商与集团公司仅能在以下情况下，移交通过云服务处理的受保护信息给外国当局或其他外国相关方： a. 法律或监管要求明确规定； b. 金融机构事先书面同意； c. 有管辖权的瑞士法院的判决； d. 瑞士主管当局授权。	客户应确保在外包协议中明确在外国诉讼的情况下，服务提供商、其分包商与集团公司仅能在以下情况下，移交通过云服务处理的受保护信息给外国当局或其他外国相关方： a. 法律或监管要求明确规定； b. 金融机构事先书面同意； c. 有管辖权的瑞士法院的判决； d. 瑞士主管当局授权。	
第 59 条	服务提供商应在与金融机构的合同中明确，服务提供商应在移交受保护信息前及时通知金融机构相关情况，以便金融机构能够行使诉讼权利，妥善处理外国当局请求。	客户应确保在外包协议中明确服务提供商应在移交受保护信息前及时通知金融机构相关情况。	
第 60 条	若由于法律强制性规定，服务提供商无法在向外国当局或其他外国相关方移交受保护信息前通知金融机构，则其应在合同范围内，实施适当的法律或保护性措施，以维护金融机构的利益。	客户应确保在外包协议中明确，如果由于法律强制性规定，服务提供商无法在向外国当局或其他外国相关方移交受保护信息前通知金融机构，则其应在合同范围内，实施适当的法律或保护性措施。	

7.8 对所使用的云服务和手段进行审计

编号	具体控制要求	客户关注点	华为云的内部实践
第 64 条	金融机构应定期审计服务提供商对适用的或合同规定的监管要求的遵守情况以及服务的履行情况。服务提供商应为金融机构的审计提供适当程度的协助。	客户应确保外包书面协议规定相应的访问权、审计权和监督权。	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。华为云会遵从与客户签订的协议中约定的要求，并会安排专人积极配合客户和监管/监管指定的代理人对华为云的审计和监督。

8 华为云如何遵从及协助客户满足瑞士《第 05/2020 号指南》

FINMA 于 2020 年 5 月 7 日发布了《第 05/2020 号指南》。该指南对所有 FINMA 所监管的机构提出了在发生具有重大影响的网络攻击事件时向监管机构报告的要求，并且明确了履行报告义务的细节规定。

金融机构在遵循上述规定时，华为云作为 CSP，可能会参与到要求所涉及的部分活动中。以下内容将总结指南中与 CSP 相关的要求，并阐述华为云作为云服务提供商如何帮助客户满足这些控制要求。

编号	具体控制要求	客户关注点	华为云的内部实践
第 3 条	1.金融机构应发现网络攻击事件并对其严重性进行初步评估后的 24 小时内通过专人通知 FINMA。详细报告应在 72 小时内通过 FINMA 的网络调查和应用平台提交。该报告应包括以下内容： a. 机构名称； b. 联系人及详细联系方式（电话和电邮地址）； c. 报告日期/时间； d. 探测到被攻击的日期/时间； e. 攻击的实际发生日期/时间（如已知）； f. 对网络攻击的描述和当前状况； g. 对网络攻击严重程度的初步评估（可选：中、高、严重等）； h. 所遭受攻击的严重性趋势（可选：减少、稳定、增加）； i. 受影响实体（金融机构或服务提供商内受影响的组织）；	客户应在规定时间内完成对网络攻击的评估并向监管机构提交包含相应内容的报告以及根本原因分析。	为配合客户满足合规要求，华为云内部制定了完善的事件管理流程。该流程清晰定义了在事件管理过程中负责各个活动的角色和职责。根据事件的影响程度和范围的不同，对事件进行优先级划分，并对不同优先级别的事件定义了不同的响应时限和解决时限。在事件发生后，华为云将根据事件对或即将对客户业务造成的影响的程度决定是否启动通报机制，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。华为云使用事件平台（CIM）记录和跟踪事件从发现到闭环的整个过程。定期会对历史事件进行趋势分析并识别类似事件，以便找到根本原因彻底解决。

	j. 受影响的保护类别（可选：保密性、完整性、可用性）； k. 受影响的关键功能/职能、业务流程或资产（如受影响的信息资源、技术基础设施、设施或人员等）； l. 受影响的客户数量（当前状况）； m. 攻击媒介（可选：电子邮件、基于 wed 端的攻击、暴力攻击、身份盗用、可移动媒体设备、设备丢失/被盗、软件漏洞利用、硬件漏洞利用等）； n. 攻击类型（需描述详情）（如 DDoS、未经授权访问、恶意软件、不正当使用技术基础设施等）； o. 金融机构在行政、具体操作和/或技术方面的应对措施，以及预期见效时间； p. 沟通方式（沟通内容、沟通对象、沟通时间等）。 2.若在提交详细报告后，出现与该网络攻击有关的新事态或进行了新评估，应在 72 小时内向 FINMA 提交新的报告。 3.针对严重程度为高与极高的网络攻击，金融机构在处理完成后，应向 FINMA 提交最终的根本原因分析报告，内容包括网络攻击成功的原因与分析、网络攻击对于遵守法规、运营以及客户的影响以及针对网络攻击所造成的后果的缓解措施。 4.针对严重程度为极高的网络攻击，金融机构还应提交危机组织能够正常运作的证据与分析。 5.针对严重程度为中等的网络攻击，金融机构提交结论性的根本原因分析即可。		

9 结语

本文描述了华为云如何为客户提供遵从瑞士金融行业监管要求的云服务，并表明华为云遵守瑞士金融市场监管局和瑞士银行家协会发布的重点监管要求，有助于客户详细了解华为云对瑞士金融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、构建和部署遵从瑞士金融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欧洲金融行业监管要求的遵从性。

10 历史版本

日期	版本	描述
2023 年 6 月	1.0	首次发布

