

1. 波兰

波兰作为欧盟成员国，其金融监管体系需遵循欧盟统一框架，同时本地监管波兰金融监管局（波兰语：Komisja Nadzoru Finansowego KNF）保留本地化执行权。

KNF曾发布受监管实体ICT风险相关指南如下，由KNF负责落地实施。2025年1月16日，**KNF宣布终止原有一系列要求，依据DORA及其配套的实施法案、监管技术标准 (RTS) 和实施技术标准 (ITS) 进行监管。**

2. 卢森堡

卢森堡作为欧盟成员国，其金融监管体系需遵循欧盟统一框架，同时本地监管卢森堡金融业管理局（Commission de Surveillance du Secteur Financier, CSSF）保留本地化执行权。1月17日，CSSF发布通知，**DORA（包括RTS、ITS等配套要求）优先于之前 CSSF 通函中的任何重叠要素，但DORA未涵盖要求仍以当前规定为主**，同时CSSF 正在更新相关文本（指南和通函），并将适时发布。

仍在实施中的要求包括：

- CSSF 20/750, Specifying the requirements regarding information and communication technology (ICT) and security risk management
- CSSF 22/806, On outsourcing arrangements (regarding ICT outsourcing arrangements)
- CSSF 24/847, On ICT-related incident reporting framework

CSSF 22/806 On outsourcing arrangements (regarding ICT outsourcing arrangements)	
原文要求	华为云遵从情况
Part I – Outsourcing arrangements - Chapter 4. Governance of outsourcing arrangements Section 4.3.2 Contractual phase	
<p>77. The outsourcing agreement shall set out:</p> <p>a. a clear description of the outsourced function to be provided;</p> <p>b. the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the In-Scope Entity;</p> <p>c. the governing law of the agreement;</p> <p>d. the parties' financial obligations;</p> <p>e. whether the sub-outsourcing, in particular, of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in points 78 to 82 that the sub-outsourcing is subject to;</p> <p>f. the location(s) (i.e. regions or countries) where the function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the In-Scope Entity if the service provider proposes to change the location(s);</p> <p>g. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in points 83 to 87;</p> <p>h. the right of the In-Scope Entity to monitor the service provider' s performance on an ongoing basis;</p> <p>i. the agreed service levels, which shall include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;</p> <p>j. the reporting obligations of the service provider to the In-Scope Entity, including the communication by the service provider of any development that may have a material impact on the service provider' s ability to effectively carry out the function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements (including the obligation to report any significant problem having an impact on the outsourced functions as well as any emergency situation) and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;</p>	<p>(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。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。</p> <p>(2) 华为云提供了线上的《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等相关信息。若是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。目前华为云欧洲站的《数据处理附录》 (https://www.huaweicloud.com/eu/declaration/sa_dpa.html) 规定了公司数据的存储、处理和管理位置【10.1 数据存储和处理设施。客户数据可在华为云或其分处理者设有设施的任何国家/地区进行处理。华为云数据中心所在的区域如下：爱尔兰 - 都柏林（华为云可能会不时更新）。】</p> <p>(3) 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。</p> <p>(3) 华为云已投保网络安全保险，将在客户要求时提供保单信息。</p>

<p>k. whether the service provider shall take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;</p> <p>l. the requirements to implement and test business contingency plans;</p> <p>m. provisions that ensure that the data that are owned by the In-Scope Entity can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;</p> <p>n. the obligation of the service provider to cooperate with the competent authorities and, where applicable, resolution authorities of the In-Scope Entity, including other persons appointed by them;</p> <p>o. for BRRD institutions, a clear reference to the national resolution authority's powers, especially to Articles 59-47 LFS, 66 and 69 of the BRRD Law, and in particular a description of the 'substantive obligations' of the contract in the sense of the Articles 59-47 LFS and 66 of the BRRD Law;</p> <p>p. the unrestricted right of In-Scope Entities and competent authorities to inspect and audit the service provider, including in case of sub-outsourcing, with regard to, at least, the critical or important outsourced function, as specified in points 88 to 100;</p> <p>q. termination rights as specified in points 101 to 103.</p>	
Sub-section 4.3.2.1 Sub-outsourcing	
<p>78. The outsourcing agreement shall specify whether or not sub-outsourcing, in particular of critical or important functions, or material parts thereof, is permitted.</p>	<p>(1) 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等要求。</p> <p>(2) 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。</p>
<p>79. If sub-outsourcing of critical or important functions is permitted, In-Scope Entities shall determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register.</p>	<p>华为云会协助客户评估拟分包的职能是否属于关键或重要部分，并配合客户将结论记录相关外包信息。</p>
<p>80. If sub-outsourcing of critical or important functions, or material parts thereof, is permitted, the written outsourcing agreement shall:</p> <p>a. specify any types of activities that are excluded from sub-outsourcing;</p> <p>b. specify the conditions to be complied with in the case of sub-outsourcing;</p> <p>c. specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the In-Scope Entity are continuously met;</p>	<p>华为云会对供应商进行定期的稽核，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。</p>

<p>d. require the service provider to obtain prior specific or general written authorisation from the In-Scope Entity before sub-outsourcing data;</p> <p>e. include an obligation of the service provider to inform the In-Scope Entity of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set shall allow the In-Scope Entity at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;</p> <p>f. ensure, where appropriate, that the In-Scope Entity has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;</p> <p>g. ensure that the In-Scope Entity has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the suboutsourcing materially increases the risks for the In-Scope Entity or where the service provider sub-outsources without notifying the In-Scope Entity.</p>	
<p>81. In-Scope Entities shall agree to sub-outsourcing critical or important functions, or material parts thereof, only if the sub-contractor undertakes to:</p> <p>a. comply with applicable laws, regulatory requirements and contractual obligations; and</p> <p>b. grant the In-Scope Entity and competent authority the same contractual rights of access and audit as those granted by the service provider.</p>	<p>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。华为云也制定了线下合同模板，可根据客户的要求，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等要求。相关分包商对于华为云及金融客户的审计要求均积极配合。</p>
<p>82. In-Scope Entities shall ensure that the service provider appropriately oversees the sub-contractors, in line with the policy defined by the In-Scope Entity. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in point 81 above would not be met, the In-Scope Entity shall exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.</p>	<p>目前华为云欧洲站的《数据处理附录》 (https://www.huaweicloud.com/eu/declaration/sa_dpa.html) 中规定了：</p> <ol style="list-style-type: none"> 1. 华为云监督其分包服务的义务【9.4 关于分处理者的义务 9.4.2 华为云将对分包给分包方的所有义务以及分包方的所有作为和不作为承担全部责任。】 2. 客户对分包更改的反对权和终止协议的权利【9.3 反对更改。客户有权在 30 天内反对更改分处理者列表，在这种情况下，客户可以将相关客户数据移动到另一个地区、终止协议或停止使用相关服务，以便被反对的分处理者不参与该客户数据的处理。客户的反对权不影响客户在本协议下的任何权利和/或义务，特别是在付款方面。】
<p>Sub-section 4.3.2.2 Security of data and systems</p>	
<p>83. The confidentiality and integrity of data and systems shall be controlled throughout the outsourcing chain. In particular, access to data and systems shall fulfil the principles of “need to</p>	<p>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</p>

<p>know” and “least privilege” , i.e. access shall only be granted to persons whose functions so require, for a specific purpose, and their privileges shall be limited to the strict necessary minimum to exercise their functions.</p>	<p>小权限，也可以通过设置登录验证策略、密码策略、访问控制列表来确保用户账户的安全。通过以上方式，实现对特权和紧急账号的有效管控。</p> <p>同时，为配合遵从监管要求，华为云还做到：</p> <ul style="list-style-type: none"> • 对于运维人员实行基于角色的访问控制，限定不同岗位不同职责的人员只能对所授权的运维目标进行特定操作，仅在员工职责所需时，对其授予特权或应急账号。 • 所有特权或应急账号的申请仅需要经过多级的评审和批准。 • 特权账号管理系统将日常或应急运维的功能账号或技术账号绑定到运维团队或个人。运维人员首先通过双因子认证接入运维环境，再集中从堡垒机跳转到目标机进行操作，堡垒机上支持强日志审计，确保运维人员在目标主机上的操作行为都可以定位到个人。 • 目标机的口令被堡垒机回收并定期更新，确保运维人员无需也无法获取口令。
<p>84. In-Scope Entities shall ensure that service providers, where relevant, comply with appropriate ICT security standards.</p>	<p>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。</p>
<p>85. Where relevant (e.g. in the context of cloud or other ICT outsourcing), InScope Entities shall define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis. Where, in the outsourcing agreement, security measures are made available by the service provider to the In-Scope Entities for personalized selection and configuration (notably for cloud outsourcing), In-Scope Entities shall ensure that proper selection and configuration take place, in line with the In-Scope Entity’ s security policy and requirements.</p>	<p>(1) 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。</p> <p>(2) 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，明确在密钥生成、传输、使用、存储、更新、备份与恢复、销毁等阶段的安管理要求。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。</p> <p>(3) 华为云操作系统、系统软件、数据库和服务器的所有配置和设置都制定了明确的安全基线要求。所有产品遵循华为云制定的网络安全红线中基线要求进行网络和系统的配置，确保限制使用不必要的功能。华为云制定了虚拟化操作系统的安全配置基线，以保证客户使用云服务时的安全性。</p>
<p>86. In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, In-Scope Entities shall adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) which shall in particular take into account point 101 c, d and e and information security considerations and comply with the provisions of points 133 to 143.</p>	<p>(1) 华为云提供了线上的《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。</p> <p>(2) 目前华为云欧洲站的《数据处理附录》(https://www.huaweicloud.com/eu/declaration/sa_dpa.html) 规定了公司数据的存储、</p>

<p>87. Without prejudice to the requirements under GDPR, In-Scope Entities, when outsourcing (in particular to third countries), shall take into account differences in national provisions regarding the protection of data. In-Scope Entities shall ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the In-Scope Entity (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).</p>	<p>处理和管理位置【10.1 数据存储和处理设施。客户数据可在华为云或其分处理者设有设施的任何国家/地区进行处理。华为云数据中心所在的区域如下：爱尔兰 - 都柏林（华为云可能会不时更新）。】</p>
<p>Sub-section 4.3.2.3 Access, information and audit rights</p>	
<p>88. In-Scope Entities shall ensure within the written outsourcing agreement that the internal audit function, the statutory auditor and the competent authority have a guaranteed access to the information relating to the outsourced functions using a risk-based approach in order to enable them to issue a well-founded opinion on the adequacy of the outsourcing. This access implies that they may also verify the relevant data kept by the service provider and, in the cases provided for in the applicable national law, have the power to perform on-site inspections of the service provider. The aforementioned opinion may, where appropriate, be based on the reports of the service provider's external auditor. The written outsourcing agreement shall also provide that the internal control functions have access to any documentation relating to the outsourced functions, at any time and without difficulty, to maintain these functions' continued ability to exercise their controls.</p>	<p>(1) 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机构或其指定的代理人对华为云的审计和监督。</p> <p>(2) 华为云制定了内审管理流程，规范内部审计原则、审计管理流程和审计频率。华为云每年由专门的审计团队执行一次内部审计工作，以检查公司内部控制体系的运行情况，评估策略、规程及配套措施和指标的符合性和有效性。此外，华为云会定期聘请独立的外部第三方提供外部审计鉴证服务，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。华为云会向最高管理层报告调查的结果和建议。管理层进行审阅并对整改情况进行跟进。</p>
<p>89. Regardless of the criticality or importance of the outsourced function, the written outsourcing agreement shall refer to the information gathering and investigatory powers of competent authorities under Articles 49, 53 and 59 LFS and Articles 31, 38 and 58-5 LPS and, where applicable, resolution authorities under Article 61(1) BRRD Law with regard to service providers located in a Member State and shall also ensure those rights with regard to service providers located in third countries.</p>	
<p>92. In-Scope Entities shall ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, their statutory auditors, competent authorities or third parties appointed by them to exercise these rights.</p>	
<p>94. Without prejudice to their final responsibility regarding outsourcing arrangements, In-Scope Entities may use: a. pooled audits organised jointly with other clients of the same service provider, and</p>	<p>华为云的云服务和平台已获得ISO27001、ISO27017、ISO27018、SOC、CSASTAR等众多国际和行业安全合规认证，涵盖信息安全、隐私保护、业务连续性管理、IT服务管理等各个领</p>

performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider; b. third-party certifications and third-party or internal audit reports, made available by the service provider.	域，致力与为各行各业的客户打造安全、可信的云服务，为客户业务赋能增值、保驾护航。并每年接受第三方审计。并提供专人协助，积极响应及配合客户方发起的审计活动。如有必要，客户可以通过官方渠道向华为云申请获取证书以及审计报告的副本。
96. In-Scope Entities shall make use of the method referred to in point 94(b) only if they: a. are satisfied with the audit plan for the outsourced function; b. ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the In-Scope Entity and the compliance with relevant regulatory requirements; c. thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete; d. ensure that key systems and controls are covered in future versions of the certification or audit report; e. are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, re-performance/verification of the evidence in the underlying audit file); f. are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place; g. have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification shall be reasonable and legitimate from a risk management perspective; and h. retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.	
97. In-Scope Entities shall, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes.	

<p>98. Before a planned on-site visit, In-Scope Entities, auditors or third parties acting on behalf of the In-Scope Entity or of the competent authority shall provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.</p>	<p>(1) 华为云会安排专人积极响应客户的要求，并提供相关材料。</p> <p>(2) 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风险评估、合同审查、绩效监控和审计监督活动。</p>
<p>99. When performing audits in multi-client environments, care shall be taken to ensure that risks to another client' s environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.</p>	<p>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，或者是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。</p>
<p>100. Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the In-Scope Entity shall verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the In-Scope Entity reviewing third-party certifications or audits carried out by service providers.</p>	<p>华为云每年定期接受专业第三方审计机构的审核。如有必要，金融机构可以通过官方渠道向华为云申请获取证书以及审计报告的副本。为了建立对华为云的信心，华为云在选择审计机构时会保证被选择的审计机构具备丰富的审计经验，能满足对外部审计方的资质要求。</p>
<p>Sub-section 4.3.2.4 Termination rights</p>	
<p>101. The outsourcing agreement shall expressly allow the possibility for the InScope Entity to terminate the arrangement in accordance with applicable law, including in the following situations: a. where the service provider of the outsourced functions is in a breach of applicable law, regulations or contractual provisions; b. where impediments capable of altering the performance of the outsourced function are identified; c. where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of subcontractors);</p>	<p>(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。如：由独立审计师对CSP的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。</p> <p>(2) 目前华为云欧洲站的《数据处理附录》 (https://www.huaweicloud.com/eu/declaration/sa_dpa.html) 中规定了对客户数据的删除和返回的规定【11. 个人数据的返回或删除】。</p>
<p>102. The outsourcing agreement shall facilitate the transfer of the outsourced function to another service provider or its re-incorporation into the In-Scope Entity, whenever the continuity or quality of the service provision are likely to be affected. To this end, the written outsourcing agreement shall: a. clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the In-Scope Entity, including the treatment of data; b. set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk</p>	<p>(3) 华为云为客户提供多种数据备份和迁移服务，可帮助客户将数据迁移至客户本地数据中心等场所。同时华为云也为客户提供多种安全机制，保障客户数据存储和传输过程中的完整性。</p> <p>(4) 在客户确认删除数据后，华为云会对指定的数据及其所有副本进行清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保</p>

<p>of disruptions; c. include an obligation of the service provider to support the In-Scope Entity in the orderly transfer of the function in the event of the termination of the outsourcing agreement; and d. without prejudice to applicable law, include a commitment for the service provider to erase the data and systems of the In-Scope Entity within a reasonable timeframe when the contract is terminated.</p>	<p>相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。</p>
Section 4.3.3 Oversight of outsourced functions	
<p>104. In-Scope Entities shall monitor, on an ongoing basis, the performance of the service providers with regard to all outsourcing arrangements on a riskbased approach and with the main focus being on the outsourcing of critical or important functions, including that the continuity of the services provided under the arrangement and the availability, integrity and security of data and information are ensured. Where the risk, nature or scale of an outsourced function has materially changed, In-Scope Entities shall reassess the criticality or importance of that function.</p>	<p>华为云遵从与客户订的协议中约定的要求，安排专人积极配合客户的需求。</p>
<p>106. In-Scope Entities shall regularly update their risk assessment in accordance with points 66 to 70 and shall periodically report to the management body on the risks identified in respect of the outsourcing of critical or important functions.</p>	<p>(1) 华为云各业务团队根据要求定期执行信息安全风险评估，网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审，确保符合公司风险管理要求。风险评估报告完成后由高级管理层进行审批。</p> <p>(2) 华为云为配合客户向管理层报告主要的网络安全风险以及补救计划，华为云会遵从与客户订的协议中约定的要求，会安排专人积极配合客户的需求。</p> <p>(3) 华为云内部制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云云环境的安全、稳定运行。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。</p>
<p>107. In-Scope Entities shall monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account points 66 to 70.</p>	<p>(4) 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法律法规、标准发生重大变化时，华为云会增加风险评估的次数。制定了风险计算和分类的流程，以确定已识别风险的可能性和影响。每种风险相关的可能性和影响是独立确定的，应考虑每种风险类别。根据风险标准，将风险降低到可接受的水平包括解决时间，都应该由管理层制定、记录和批准。网络安全与用户隐私办公室定期组织信息安全评估与重大事件回溯工作专家组会议，识别有关的网络安全风险，并对风险处置跟进过程进行定期评审。</p> <p>(5) 华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。</p>

<p>108. In-Scope Entities shall ensure, on an ongoing basis, that outsourcing arrangements, with the main focus being on outsourced critical or important functions, meet appropriate performance and quality standards in line with their policies by: a. ensuring that they receive appropriate reports from service providers; b. evaluating the performance of service providers using tools such as key performance indicators, key control indicators, service delivery reports, self-certification and independent reviews; and c. reviewing all other relevant information received from the service provider, including reports on business continuity measures and testing.</p>	<p>(1) 华为云内部制定了完善的信息安全风险管理机制，定期进行风险评估和合规审查，以实现华为云环境的安全、稳定运行。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法律法规、标准发生重大变化时，华为云会增加风险评估的次数。华为云对外包商进行严格的安全管理，定期对供应商进行审计和评估。</p> <p>(2) 为配合客户满足合规要求，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。华为云已与合作伙伴联合推出了主机入侵检测、Web 应用防火墙、主机漏洞检测、网页 防篡改服务及渗透测试等服务，提升了华为云的安全检测、感知及防御能力。</p> <p>(3) 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。</p>
<p>109. In-Scope Entities shall take appropriate measures if they identify shortcomings in the provision of the outsourced function. In particular, In-Scope Entities shall follow up on any indications that service providers may not be carrying out the outsourced critical or important function effectively or in compliance with applicable laws and regulatory requirements. If shortcomings are identified, In-Scope Entities shall take appropriate corrective or remedial actions. Such actions may include terminating the outsourcing agreement, with immediate effect, if necessary.</p>	<p>华为云为配合客户向管理层报告主要的网络安全风险以及补救计划，华为云应遵从与客户订的协议中约定的要求，安排专人积极配合客户的需求。</p>
<p>Section 4.3.4 Exit plans</p>	
<p>112. In-Scope Entities shall ensure that they are able to exit outsourcing arrangements without undue disruption to their business activities, without limiting their compliance with regulatory requirements and without any detriment to the continuity and quality of its provision of services to clients. To achieve this, they shall: a. develop and implement exit plans that are comprehensive, documented and, where appropriate, sufficiently tested (e.g. by carrying out an analysis of the potential costs, impacts, resources and timing implications of transferring an outsourced service to an alternative provider); and b. identify alternative solutions and develop transition plans to enable InScope Entities to remove outsourced functions and data from the service provider and transfer them to alternative providers or back to the In-Scope Entity or to take other measures that ensure the continuous provision of the critical or important function or business activity in a controlled and sufficiently tested manner, taking</p>	<p>(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。如：由独立审计师对CSP的运营进行审计、华为云若将服务分包给其他供应商的条件和责任等。</p> <p>(2) 目前华为云欧洲站的《数据处理附录》 (https://www.huaweicloud.com/eu/declaration/sa_dpa.html) 中规定了对客户数据的删除和返回的规定【11. 个人数据的返回或删除】。</p> <p>华为云为客户提供多种数据备份和迁移服务，可帮助客户将数据迁移至客户本地数据中心等场所。同时华为云也为客户提供多种安全机制，保障客户数据存储和传输过程中的完整性。</p>

into account the challenges that may arise because of the location of data and taking the necessary measures to ensure business continuity during the transition phase.	(3) 在客户确认删除数据后，华为云会对指定的数据及其所有副本进行清除，首先删除客户与数据之间的索引关系，并在将内存、块存储等存储空间进行重新分配前进行清零操作，确保相关的数据和信息不可还原。对于物理存储介质报废的情况，华为云通过对存储介质进行消磁、折弯或破碎等方式进行数据清除，确保其上的数据无法恢复。
113. When developing exit plans, In-Scope Entities shall: a. define the objectives of the exit plan; b. perform a business impact analysis that is commensurate with the risk of the outsourced processes, services or activities, with the aim of identifying what human and financial resources would be required to implement the exit plan and how much time it would take; c. assign roles, responsibilities and sufficient resources to manage exit plans and the transition of activities; d. define success criteria for the transition of outsourced functions and data; and e. define the indicators to be used for the monitoring of the outsourcing arrangement (as outlined under points 104 to 110) including indicators based on unacceptable service levels that shall trigger the exit.	