CSSF 22/806 On outsourcing arrangements (regarding ICT outsourcing arrangements)	
Original Requirements	**Huawei Cloud's Compliance Status**
Part I – Outsourcing arrangements - Chapter 4. Governance of outsourcing arrangements **Section 4.3.2 Contractual phase**	
77. The outsourcing agreement shall set out: a. a clear description of the outsourced function to be provided; 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; c. the governing law of the agreement; d. the parties' financial obligations; 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; 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); g. where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in points 83 to 87; h. the right of the In-Scope Entity to monitor the service provider' s performance on an ongoing basis; 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; 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;	(1) Huawei Cloud provides online binding agreements including the Huawei Cloud Customer Agreement and Service Level Agreement (SLA), which define the scope of services, performance standards, and Huawei Cloud's operational responsibilities. Offline contract templates are also available for customization to meet specific client requirements. These documents incorporate Huawei Cloud's security measures, such as encryption, access control, incident management, configuration governance, and third-party security audits. Huawei Cloud commits to continuously updating and enhancing these measures to ensure the security of customer data. (2) Huawei Cloud publishes a Data Processing Addendum that discloses permitted data center locations for customer deployment. Current European operations specify data processing facilities in Dublin, Ireland (subject to Huawei Cloud updates). The document explicitly states: "Customer data may be processed in any country/region where Huawei Cloud or its subprocessors operate facilities" (Section 10.1 Data Storage and Processing Facilities). Changes to data center/operations hub locations during deployment trigger timely disclosure obligations. Upon client request, Huawei Cloud will also disclose information related to critical subcontractors.

k. whether the service provider shall take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested; l. the requirements to implement and test business contingency plans; 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; 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; o. for BRRD institutions, a clear reference to the national resolution authority' s30 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. 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; q. termination rights as specified in points 101 to 103.	(3) Upon termination of service agreements, customers may utilize Huawei Cloud's Cloud Data Migration (CDM) service to transfer data across heterogeneous environments, including databases, data warehouses, and file systems. The service supports cross-platform migrations to address scenarios such as cloud adoption, inter-cloud data exchange, and local data center repatriation. (4) Huawei Cloud maintains enterprise-grade cybersecurity insurance policies. Policy details will be provided to clients upon formal request.
Sub-section 4.3.2.1 Sub-outsourcing	
78. The outsourcing agreement shall specify whether or not sub-outsourcing, in particular of critical or important functions, or material parts thereof, is permitted.	(1) Huawei Cloud's online Huawei Cloud Customer Agreement defines security responsibilities between customers and Huawei Cloud, while the Service Level Agreement (SLA) establishes service performance benchmarks. Offline contract templates are also available for customization based on client requirements, including provisions that mandate notification to customers when Huawei Cloud engages subcontractors and ensure Huawei Cloud's full accountability for subcontracted services. (2) Huawei Cloud has established a comprehensive supplier management framework that enforces security requirements across supplier product development lifecycles and internal governance processes. This includes regular audits of suppliers, mandatory Network Security Agreements for cybersecurity vendors, and continuous

	monitoring of service quality through performance-based scoring. Suppliers with subpar security performance are subject to collaboration downgrade mechanisms to ensure compliance with Huawei Cloud's security standards.
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.	Huawei Cloud assists clients in evaluating whether the functions intended for outsourcing are classified as critical or essential, and collaborates with clients to document the relevant outsourcing information.
80. If sub-outsourcing of critical or important functions, or material parts thereof, is permitted, the written outsourcing agreement shall: a. specify any types of activities that are excluded from sub-outsourcing; b. specify the conditions to be complied with in the case of sub-outsourcing; 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; d. require the service provider to obtain prior specific or general written authorisation from the In-Scope Entity before sub-outsourcing data; 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; 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; 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.	Huawei Cloud conducts regular audits of suppliers, requires cybersecurity vendors to sign Network Security Agreements, and maintains continuous monitoring of service quality through performance-based scoring. Suppliers with subpar security performance are subject to collaboration downgrade mechanisms to ensure compliance with Huawei Cloud's security standards.
81. In-Scope Entities shall agree to sub-outsourcing critical or important functions, or material parts thereof, only if the sub-contractor undertakes to: a. comply with applicable laws, regulatory requirements and contractual obligations; and	Huawei Cloud outlines security responsibilities between customers and Huawei Cloud in the online Huawei Cloud Customer Agreement, while the Service Level Agreement (SLA) establishes performance benchmarks for cloud services. Offline contract templates are also available for customization, which may include provisions requiring

b. grant the In-Scope Entity and competent authority the same contractual rights of access and audit as those granted by the service provider.	Huawei Cloud to notify customers when engaging subcontractors and to assume full accountability for subcontracted services. Subcontractors involved in Huawei Cloud and financial sector projects collaborate proactively with audit requirements from both Huawei Cloud and client organizations.
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.	Huawei Cloud's Data Processing Addendum (European Site) Relevant Provisions Extracted from https://www.huaweicloud.com/eu/declaration/sa_dpa.html 9.4 Obligations Regarding Sub-Processors Huawei Cloud retains full liability for all obligations subcontracted to Sub-Processors and for all acts and omissions performed by Sub-Processors in relation to the processing of Customer Data under the terms of this Addendum. 9.3 Right to Object to Sub-Processor Changes Customers are granted the right to object to modifications in the Sub-Processors List within 30 calendar days of notification, and in such cases, Huawei Cloud enables customers to migrate relevant Customer Data to another designated region, terminate the Agreement, or cease using the affected Service(s) to ensure the objected Sub-Processor no longer processes the Customer Data. This objection right does not prejudice the Customer’ s other rights and obligations under the Agreement, particularly payment liabilities.
Sub-section 4.3.2.2 Security of data and systems	
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 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.	HUAWEI CLOUD's Identity and Access Management (IAM) provides customers with cloud resource access control. Through IAM, customer administrators can manage user accounts and control the operational permissions these accounts have over resources under the customer's name. When multiple users collaborate on resource operations within an enterprise, IAM helps avoid sharing account credentials among

	users by enabling on-demand assignment of least privileges. It also ensures account security through configurable login verification policies, password policies, and access control lists (ACLs). These mechanisms facilitate effective governance over privileged and emergency accounts. To comply with regulatory requirements, HUAWEI CLOUD implements additional measures: ● Role-based access control for operation and maintenance (O&M) personnel, restricting staff with different roles and responsibilities to authorized operations on specific O&M targets. Privileged or emergency accounts are granted only when necessary for job functions. ● All privileged or emergency account requests require multi-level review and approval processes. ● The privileged account management system binds functional or technical accounts (whether for routine or emergency O&M) to O&M teams or individuals. O&M personnel must first access the O&M environment through two-factor authentication, then centrally connect via bastion hosts to target machines. The bastion hosts support robust log auditing to ensure all operations on target hosts can be traced to individual users. ● The passwords of target machines are reclaimed by bastion hosts and regularly updated, ensuring O&M personnel neither require nor can obtain direct password access.

84. In-Scope Entities shall ensure that service providers, where relevant, comply with appropriate ICT security standards.	Huawei Cloud adheres to international standards such as ISO/IEC 27001, ISO/IEC 20000, and ISO 22301 to establish comprehensive Information Security Management Systems (ISMS), IT Service Management Systems, and Business Continuity Management Systems (BCMS). These frameworks are rigorously implemented in daily operations to ensure alignment with global best practices. Additionally, Huawei Cloud conducts annual risk assessments and management reviews to identify operational gaps within these systems. Corrective actions are systematically executed to address identified issues, driving continuous improvement of the management frameworks.
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.	(1) The online HUAWEI CLOUD Customer Agreement delineates security responsibilities between customers and HUAWEI CLOUD, while the HUAWEI CLOUD Service Level Agreement specifies the service levels provided by HUAWEI CLOUD. (2) HUAWEI CLOUD has formulated and implemented Key Management Security Specifications to govern security throughout the key lifecycle. These specifications define security requirements for key generation, transmission, usage, storage, update, backup & recovery, and destruction. HUAWEI CLOUD employs multiple safeguards including online redundant storage of customer master keys, multiple physical offline backups of root keys, and regular backup mechanisms to ensure key durability. (3) HUAWEI CLOUD establishes explicit security baseline requirements for operating systems, system software, databases, and server configurations. All products adhere to network and system configuration standards defined in HUAWEI CLOUD's cybersecurity baselines, ensuring the restriction of unnecessary functionalities. Additionally, HUAWEI CLOUD enforces security configuration baselines for virtualized operating systems to guarantee the safety of cloud services for customers.

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.	(1) HUAWEI CLOUD provides an online Data Processing Addendum that explicitly discloses the locations of data centers available for customer deployment. If the locations of data centers or operational centers change during customer deployment, HUAWEI CLOUD will promptly update this information. Additionally, HUAWEI CLOUD discloses relevant details to customers upon request, such as information pertaining to critical subcontractors. (2) The Data Processing Addendum for HUAWEI CLOUD's European region currently stipulates the storage, processing, and management locations of company data: 【10.1 Data Storage and Processing Facilities. Customer data may be processed in any country/region where HUAWEI CLOUD or its sub-processors maintain facilities. HUAWEI CLOUD's data centers are located in the following region: Ireland – Dublin (subject to updates by HUAWEI CLOUD from time to time).】
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).	
Sub-section 4.3.2.3 Access, information and audit rights	
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.	(1) HUAWEI CLOUD commits to customers' audit and oversight rights in agreements signed with customers based on actual conditions. HUAWEI CLOUD complies with requirements stipulated in customer agreements and assigns dedicated personnel to actively cooperate with audits and supervision conducted by customers, regulatory authorities, or their designated representatives. (2) Huawei Cloud has established internal audit management procedures to standardize audit principles, management workflows, and audit frequency. Annually, a dedicated audit team conducts comprehensive internal audits to evaluate the
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.	operational effectiveness of the company's internal control systems. These audits assess the compliance and effectiveness of strategies, protocols, supporting measures, and performance metrics in alignment with Huawei Cloud's governance objectives. Additionally, Huawei Cloud engages independent external third-party auditors to perform periodic external audit assurance services. These auditors independently evaluate the confidentiality, integrity, availability, and security of information and resources through regular security assessments and compliance audits (e.g., Service Organization Controls (SOC), ISO standards, Payment Card Industry Data Security Standard (PCI DSS)). Such evaluations ensure objective scrutiny of risk management content and processes. Findings and recommendations from both internal and external audits are reported to senior management. Management reviews the outcomes and follows up on corrective actions to address identified gaps, ensuring continuous improvement of the governance framework.
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.	
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 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.	Huawei Cloud's cloud services and platforms have obtained numerous international and industry-recognized security compliance certifications, including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC, CSA STAR, and others. These certifications comprehensively cover domains such as information security, privacy protection, business continuity management, and IT service management. Huawei Cloud is
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.	dedicated to building secure and trustworthy cloud services for customers across industries, empowering their business growth and providing robust protection. Huawei Cloud undergoes annual independent third-party audits to validate its compliance and security posture. Additionally, Huawei Cloud offers dedicated support teams to promptly respond to and actively collaborate with customers initiating audit activities. If required, customers may submit formal requests through official channels to obtain copies of certification documents or audit reports.
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.	Huawei PSIRT and Huawei Cloud security operations team have established a comprehensive mechanism for vulnerability perception, handling, and external disclosure. At the same time, Huawei Cloud actively implements security quality assurance work for cloud products and platforms, and conducts internal and third-party penetration testing and security assessments annually to ensure the security of Huawei Cloud's cloud environment.
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.	(1) Huawei Cloud will assign dedicated personnel to actively respond to customer requirements and provide relevant materials. (2) Huawei Cloud undergoes regular audits by professional third-party audit institutions annually, and provides assigned personnel to actively assist, respond to,

	and cooperate with customer-initiated activities such as risk assessment, contract review, performance monitoring, and audit supervision.
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.	Huawei Cloud explicitly states in its user agreements that it will not access or use user content, except for providing necessary services to users or complying with laws, regulations, or binding orders from governmental authorities, and strictly adheres to all applicable legal requirements regarding data security and privacy protection for customers. Additionally, contracts signed with customers clearly define Huawei Cloud’ s liability to customers in cases of breaches of confidentiality clauses. Furthermore, all Huawei Cloud service products and components have been designed and implemented with isolation mechanisms from the initial phase to prevent intentional or unintentional unauthorized access or tampering between customers, thereby reducing the risk of data leakage. Taking data storage as an example, Huawei Cloud’ s block storage, object storage, and file storage services all incorporate customer data isolation as a critical feature.
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.	Huawei Cloud undergoes regular audits by professional third-party audit institutions annually. If necessary, financial institutions may apply through official channels to Huawei Cloud for copies of certificates and audit reports. To instill confidence in Huawei Cloud, Huawei Cloud ensures that the selected audit institutions possess extensive auditing experience and meet the qualification requirements for external auditors.
Sub-section 4.3.2.4 Termination rights	
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);	(1) HUAWEI CLOUD provides online HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which define service scope, service levels, and HUAWEI CLOUD’ s responsibilities. Additionally, HUAWEI CLOUD offers offline contract templates customizable to meet diverse customer requirements, such as clauses for independent audits of CSP operations and terms governing subcontracting to third-party suppliers, including associated conditions and liabilities.
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 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.	(2) The Data Processing Addendum for HUAWEI CLOUD’ s European region specifies provisions for data deletion and return in its [11. Return or Deletion of Personal Data] section. (3) HUAWEI CLOUD offers multiple data backup and migration services to assist customers in transferring data to on-premises data centers or other designated locations. Concurrently, HUAWEI CLOUD implements robust security mechanisms to ensure the integrity of customer data during storage and transmission. (4) After the customer confirms data deletion, Huawei Cloud will erase the specified data and all its copies by first deleting the index relationships between the customer and the data, and then performing a zeroing process on memory, block storage, and other storage spaces before reallocating them, ensuring that the associated data and information become irretrievable. For physical storage media disposal, Huawei Cloud employs data eradication methods such as demagnetization, bending, or crushing of the storage media to ensure that data stored on them cannot be recovered.
Section 4.3.3 Oversight of outsourced functions	
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.	Huawei Cloud complies with the requirements stipulated in the agreements signed with customers and assigns dedicated personnel to actively cooperate with customer needs.
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.	(1) HUAWEI CLOUD business teams periodically conduct information security risk assessments as required. The Cybersecurity and User Privacy Office regularly convenes expert group meetings for information security evaluations and major incident retrospectives to identify cybersecurity risks, review risk remediation follow-up

107. In-Scope Entities shall monitor and manage their internal concentration risks caused by outsourcing arrangements, taking into account points 66 to 70.	processes, and ensure compliance with corporate risk management requirements. Completed risk assessment reports are approved by senior management. (2) To support customers in reporting major cybersecurity risks and remediation plans to their management, HUAWEI CLOUD complies with requirements stipulated in customer agreements and assigns dedicated personnel to actively collaborate with customers. (3) HUAWEI CLOUD maintains a comprehensive internal information security risk management mechanism, conducting regular risk assessments and compliance reviews to ensure secure and stable operations of its cloud environment. HUAWEI CLOUD adheres to Huawei’ s corporate information security risk management framework, which strictly defines risk management scope, organizational responsibilities, and standardized processes. (4) HUAWEI CLOUD performs annual risk assessments and increases assessment frequency under specific circumstances, such as major system changes, significant business transformations, or updates to laws, regulations, or standards. The company implements risk calculation and classification processes to determine the likelihood and impact of identified risks. Each risk’ s probability and impact are independently evaluated across risk categories. Management defines, documents, and approves risk mitigation plans to reduce risks to acceptable levels, including resolution timelines. The Cybersecurity and User Privacy Office periodically organizes expert meetings to assess cybersecurity risks and review risk remediation progress.

	(5) HUAWEI CLOUD enforces strict security management for third-party vendors, including regular audits and evaluations of suppliers.
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.	(1) Huawei Cloud has established a comprehensive information security risk management framework, including regular risk assessments and compliance reviews, to ensure the secure and stable operation of its cloud environment. Huawei Cloud adheres to Huawei’ s Information Security Risk Management Framework, which strictly defines the scope, organizational structure, and standardized procedures for risk management. Huawei Cloud conducts annual risk assessments and increases the frequency when significant changes occur in information systems, business operations, or regulatory standards. Additionally, Huawei Cloud enforces stringent security management for third-party vendors through regular audits and evaluations of suppliers. (2) To support customers in meeting compliance requirements, Huawei Cloud periodically performs internal and third-party penetration testing and security assessments to monitor, identify, and mitigate security threats, ensuring the security of cloud services. Huawei Cloud has collaborated with partners to launch services such as Host-based Intrusion Detection, Web Application Firewall (WAF), Host Vulnerability Detection, Webpage Anti-Tampering Service, and Penetration Testing. These services

	enhance Huawei Cloud’ s capabilities in security detection, threat awareness, and defense mechanisms. (3) Huawei Cloud utilizes a Big Data Security Analytics System to centrally analyze alerts and logs from various security devices. Security incidents are classified based on their impact levels on customer operations, triggering a customer notification process to inform clients. Upon resolution of an incident, Huawei Cloud provides detailed incident reports to customers based on specific circumstances.
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.	To assist customers in reporting major cybersecurity risks and remediation plans to their management, Huawei Cloud shall comply with stipulated requirements in agreements with customers and assign dedicated personnel to actively cooperate with customer needs.
Section 4.3.4 Exit plans	
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	(1) HUAWEI CLOUD provides online HUAWEI CLOUD Customer Agreement and HUAWEI CLOUD Service Level Agreement, which specify service offerings, service levels, and HUAWEI CLOUD’ s responsibilities. Additionally, HUAWEI CLOUD offers customizable offline contract templates tailored to diverse customer needs, including provisions such as independent audits of CSP operations and terms governing

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.	subcontracting conditions and liabilities when services are delegated to third-party suppliers. (2) The Data Processing Addendum for HUAWEI CLOUD’ s European region outlines requirements for data deletion and return under its [11. Return or Deletion of Personal Data] section. HUAWEI CLOUD provides multiple data backup and migration services to assist customers in migrating data to on-premises data centers or other designated locations, alongside implementing robust security mechanisms to ensure data integrity during storage and transmission. (3) Upon client confirmation of data deletion, Huawei Cloud will erase the designated data and all its copies by first deleting the indexing relationship between the customer and the data, followed by performing a zero-fill operation on memory and block storage before reallocating storage space to ensure data irrecoverability. For decommissioned physical storage media, Huawei Cloud employs methods such as demagnetization, bending, or crushing to permanently destroy data and prevent recovery.
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.	