HUAWEI CLOUD User Guide to Financial Services Regulations & Guidelines in Switzerland

Issue 1.0

Date 2023-05-29

HUAWEI CLOUD

HUAWEI

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between HUAWEI CLOUD and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Sparkoo Technologies Ireland Co., Ltd.

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

Website: https://www.huaweicloud.com/eu/

Contents

1 Overview

1.1 Background and Purpose of Publication

With the development of technology, the use of cloud computing technologies and services has become the norm in Switzerland financial institutions. Cloud computing brings great convenience to the development of financial institutions and creates a more complex business operation environment for financial institutions. In order to regulate the use of information technology in the financial industry, the Swiss Financial Market Regulatory Authority and the Swiss Bankers Association have issued a series of regulatory regulations on cyber security and information technology risk management of Swiss financial institutions.

As a cloud service provider, HUAWEI CLOUD is committed to helping financial customers meet these regulatory requirements and continuously providing financial customers with cloud services and service operating environments that comply with financial industry standards. This document describes how HUAWEI CLOUD will help financial institutions meet the regulatory requirements when using cloud services.

1.2 Introduction of Applicable Financial Regulatory Requirements

The Swiss Financial Markets Supervisory Authority (FINMA) is the Swiss financial industry regulator responsible for ensuring the effective functioning of the Swiss financial markets; The Swiss Bankers Association (SBA) is the world's largest banking industry association, its members include Swiss banks, auditors and brokers, and has a significant influence in Switzerland and the international financial community.

- **Circular 2018/3 Outsourcing**: FINMA issued this circular on 21 September 2017, which sets out the requirements that banks, brokers and insurance companies must comply with when performing significant functions outsourcing activities.
- **Circular 2023/1 Operational Risks and Resilience - Banks**: FINMA issued this Circular on 7 December 2022, which comprehensively revised Circular 2008/21 Operational Risks - Banks and improved regulatory practices in relation to operational risk management. The principle of operation flexibility is added. Regulatory areas include overall operational risk management, ICT risk management, network risk management, key risk management, business continuity management, cross-border transaction risk management, and operational flexibility assurance.
- **Cloud Guidelines**: The SBA released the guidelines on June 1, 2020, identifying four key areas related to the delivery of banking and financial services through cloud technologies, including governance, data and data security, authorities and proceedings, and audit of cloud services and means used. The guide provides recommendations on

how to manage these areas. These recommendations are not legally binding. Banks can apply this guidance as a best practice given their size and complexity of their business model.

- **Guidance 05/2020**: FINMA published this guidance on May 7, 2020. There is a requirement for all FINMA-supervised institutions to report to regulators in the event of a material cyberattack, and details of reporting obligations are specified.

1.3 Definition

- **HUAWEI CLOUD**

  HUAWEI CLOUD is the cloud service brand of the HUAWEI marquee, committed to providing stable, secure, reliable, and sustainable cloud services.

- **Customer**

  Refers to registered users who have entered into commercial relations with HUAWEI CLOUD

- **Outsourcing**

  Outsourcing occurs when financial institutions mandate a service provider to perform all or part of a function that is significant to the financial institution’s business activities independently and on an ongoing basis.

- **Significant functions**

  Significant functions are those that have a material effect on compliance with the aims and regulations of financial market legislation.

- **Critical data**

  Critical data are data that, in view of the financial institution's size, complexity, structure, risk profile and business model, are of such crucial significance that they require increased security measures. These are data that are crucial for the successful and sustainable provision of the institution's services or for regulatory purposes.

- **Critical processes**

  Critical processes are processes whose significant disruption endanger the provision of critical functions. They are part of the critical functions.

- **ICT**

  ICT refers to the physical and logical (electronic) architecture of IT and communication systems, the individual hardware and software assets, networks, data and operating environments.

- **Client identifying data (CID)**

  CID refers to client data that reflects personal data and identifies the client involved.

- **Protected information**

  Protected information means CID, personal data and other information and data designated by the institution as requiring to be treated confidentially.

- **Significant subcontractors**

  Significant subcontractors means subcontractors performing significant functions and subcontractors deemed significant by financial institutions

2 HUAWEI CLOUD Security and Privacy Compliance

HUAWEI CLOUD inherits Huawei's comprehensive management system and leverages its experience in IT system construction and operation, actively managing and continuously improving the development, operation and maintenance of cloud services. To date, HUAWEI CLOUD has received a number of international and industry security compliance certifications ensuring the security and compliance of businesses deployed by cloud service customers.

HUAWEI CLOUD services and platforms have obtained the following certifications:

Global Standard Certification

Certification	Description
ISO 20000-1:2011	ISO 20000 is an international recognized information technology Service Management System (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers (CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO 27001:2013	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
SOC audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers.

PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
CSA STAR Gold Certification	The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
International Common Criteria EAL 3+ Certification	Common Criteria certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD Fusion Sphere passed Common Criteria EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide.
ISO 27018:2014	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that HUAWEI CLOUD has a complete personal data protection management system and is in the global leading position in data security management.
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms HUAWEI CLOUD’s implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
ISO 27701:2019	ISO 27701 specifics requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
M&O Certification	Uptime Institute is a globally recognized data center standardization organization and authoritative professional certification organization. HUAWEI CLOUD data center has adopted the world's top data center infrastructure O&M certification (M&O certification) issued by Uptime Institute. The adoption of M&O certification indicates that HUAWEI CLOUD data center O&M management is at the leading level in the world.
NIST CSF	NIST CSF consists of three parts: the Framework Core, the Implementation Tiers and the Framework Profiles. The Framework Core consists of five concurrent and continuous

	Functions—Identify Protect Detect Respond Recover. This capability Framework covers the entire cybersecurity process before, during, and after the event, helping enterprises proactively identify, prevent, detect, and respond to security risks.
PCI 3DS	The PCI 3DS standard is designed to protect 3DS environments that perform specific 3DS functions or store 3DS data and support 3DS implementation. Passing the PCI 3DS certification shows that HUAWEI CLOUD complies with security standards in the process, flow, and personnel management of the 3D protocol execution environment.

Regional Standard Certification

Certification	Description
Classified Cybersecurity Protection of China's Ministry of Public Security (China)	Classified Cybersecurity Protection issued by China's Ministry of Public Security is used to guide organizations in China through cybersecurity development. Today, it has become the general security standard widely adopted by various industries throughout China. HUAWEI CLOUD has passed the registration and assessment of Classified Cybersecurity Protection Class 3. In addition, key HUAWEI CLOUD regions and nodes have passed the registration and assessment of Classified Cybersecurity Protection Class 4.
Singapore MTCS Level 3 Certification (Singapore)	The Multi-Tier Cloud Security (MTCS) specification is a standard developed by the Singapore Information Technology Standards Committee. This standard requires cloud service providers (CSPs) to adopt sound risk management and security practices in cloud computing. HUAWEI CLOUD Singapore has obtained the highest level of MTCS security rating (Level 3).
Gold O&M (TRUCS) (China)	The Gold O&M certification is designed to assess the O&M capability of cloud service providers who have passed TRUCS certification. This certification confirms that HUAWEI CLOUD services operate a sound O&M management system that satisfies the cloud service O&M assurance requirements specified in Chinese certification standards.
Certification for the Capability of Protecting Cloud Service User Data (TRUCS) (China)	This certification evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking.

ITSS Cloud Computing Service Capability Evaluation by the Ministry of Industry and Information Technology (MIIT) (China)	ITSS cloud computing service capability evaluation is based on Chinese standards such as the General Requirements for Cloud Computing and Cloud Service Operations. It is the first hierarchical evaluation mechanism in China's cloud service/cloud computing domain. Huawei private and public clouds have obtained cloud computing service capability level-1 (top level) compliance certification.
TRUCS (China)	Trusted Cloud Service (TRUCS) is one of the most authoritative public domain assessments in China. This assessment confirms that HUAWEI CLOUD complies with the most detailed standard for cloud service data and service assurance in China.
Cloud Service Security Certification Cyberspace Administration of China (CAC) (China)	This certification is a third-party security review conducted by the Cyberspace Administration of China according to the Security Capability Requirements of Cloud Computing Service. HUAWEI CLOUD e-Government Cloud Service Platform has passed the security review (enhanced level), indicating that Huawei e-Government cloud platform was recognized for its security and controllability by China's top cybersecurity management organization.

Currently, Sparkoo (Ireland) has also received a number of international and industry security compliance certifications, including:

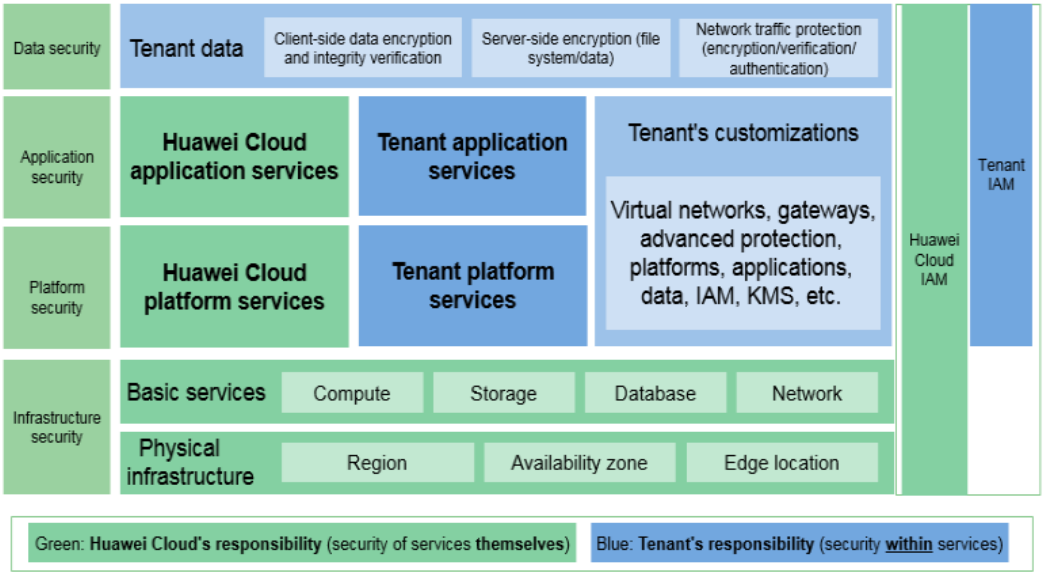
Certification	Description
ISO 27001:2013	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that Sparkoo has achieved internationally recognized best practices in information security management.
ISO 27018:2014	ISO 27018 is the first international code of conduct that focuses on personal data protection in the cloud. This certification indicates that Sparkoo has a complete personal data protection management system and is in the global leading position in data security management.
ISO 29151:2017	ISO 29151 is an international practical guide to the protection of personal identity information. The adoption of ISO 29151 confirms Sparkoo's implementation of internationally recognized management measures for the entire lifecycle of personal data processing.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that Sparkoo offers a complete personal data

	protection system to ensure personal data security.
ISO 27701:2019	ISO 27701 specifics requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that Sparkoo operates a sound system for personal data protection.
ISO 20000-1:2011	ISO 20000 is an international recognized information technology Service Management System (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers (CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO 22301:2012	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Gold Certification	The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing service providers to demonstrate their service maturity.
PCI DSS Certification	Payment Card Industry Data Security Standard (PCI DSS) is the global card industry security standard, jointly established by five major international payment brands: JCB, American Express, Discover, MasterCard and Visa. It is the most authoritative and strict financial institution certification in the world.
SOC audit	The SOC audit report is an independent audit report issued by a third-party auditor based on the relevant guidelines developed by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers.
NIST CSF	NIST CSF consists of three parts: the Framework Core, the Implementation Tiers and the Framework Profiles. The Framework Core consists of five concurrent and continuous Functions—Identify Protect Detect Respond Recover. This capability Framework covers the entire cybersecurity process before, during, and after the event, helping enterprises proactively identify, prevent, detect, and respond to security risks.

For more information on HUAWEI CLOUD security compliance and downloading relevant compliance Certification please refer to the official website of HUAWEI CLOUD "**Trust Center - Compliance**"

3 HUAWEI CLOUD Security Responsibility Sharing Model

Due to the complex cloud service business model, cloud security is not the sole responsibility of one single party, but requires the joint efforts of both the customer and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help customers to understand the security responsibility scope for both parties and ensure the coverage of all areas of cloud security. Below is an overview of the responsibilities sharing model between the customer and HUAWEI CLOUD:



As shown in the above model, the privacy protection responsibilities are distributed between HUAWEI CLOUD and customers as below:

HUAWEI CLOUD: The primary responsibilities of HUAWEI CLOUD are developing and operating the physical infrastructure of HUAWEI CLOUD data centers; the IaaS, PaaS, and SaaS services provided by HUAWEI CLOUD; and the built-in security functions of a variety of services. Furthermore, HUAWEI CLOUD is also responsible for the secure design, implementation, and O&M of the multi-layered defense-in-depth, which spans the physical, infrastructure, platform, application, and data layers, in addition to the identity and access management (IAM) cross layer function.

Customer: The primary responsibilities of the customers are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a customer subscribes on HUAWEI CLOUD, including its customization of HUAWEI CLOUD services according to its needs as well as the O&M of any platform, application, and IAM services that the customer deploys on HUAWEI CLOUD. At the same time, the customer is also responsible for the customization of the security settings at the virtual network layer, the platform layer, the application layer, the data layer,

and the cross-layer IAM function, as well as the tenant's own in-cloud O&M security and the effective management of its users and identities.

For details on the security responsibilities of both Customers and HUAWEI CLOUD, please refer to the **HUAWEI CLOUD Security White Paper** released by HUAWEI CLOUD.

4 HUAWEI CLOUD Global Infrastructure

HUAWEI CLOUD operates services in many countries and regions around the world. The HUAWEI CLOUD infrastructure is built around Regions and Availability Zones (AZ). Compute instances and data stored in HUAWEI CLOUD can be flexibly exchanged among multiple regions or multiple AZs within the same region. Each AZ is an independent, physically isolated fault maintenance domain, Users can and should take full advantage of all these regions and AZs in their planning for application deployment and operations in HUAWEI CLOUD. Distributed deployment of an application across a number of AZs provides a high degree of assurance for normal application operations and business continuity in most outage scenarios (including natural disasters and system failures). For current information on HUAWEI CLOUD Regions and Availability Zones, please refer to the official website of HUAWEI CLOUD "**Worldwide Infrastructure**".

5 How HUAWEI CLOUD Meets and Assists Customers to Meet Circular 2018/3 Outsourcing

FINMA issued Circular 2018/3 Outsourcing on 21 September 2017, which sets out the requirements that banks, brokers and insurance companies must comply with when performing significant functions outsourcing activities.

When financial institutions comply with the above provisions, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following content will summarize the requirements related to cloud service providers in the guide, and explain how HUAWEI CLOUD, as a cloud service provider, helps customers meet these control requirements.

5.1 Selection, Instruction and Monitoring of the Service Provider

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
17	When selecting a service provider, financial institutions should give due consideration to and review their professional capabilities and financial and human resources.	Customers should consider the professional capabilities, human resources and financial situation of the service provider in due diligence.	HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements and due diligence initiated by the customer. HUAWEI CLOUD has passed multiple international security and privacy protection certifications, including ISO 27001, ISO 27017, ISO 27018, SOC, and CSA STAR, and is audited by a third party every year. ●Professional capabilities: HUAWEI CLOUD complies with international standards such as ISO27001, ISO20000, and ISO22301 to establish a

			comprehensive information security management system, IT service management system, and business continuity management system, and implements the system requirements in daily operations. In addition, HUAWEI CLOUD regularly conducts risk assessment and management review activities every year to identify problems during system operation, implement rectification, and promote continuous improvement of the management system. ●Personnel management: HUAWEI CLOUD strictly implements the long-standing effective personnel and personnel management mechanism. All HUAWEI CLOUD employees, partners, and external consultants must comply with Huawei security policies and receive security training to integrate security concepts into the entire organization. HUAWEI CLOUD rewards employees who actively implement cyber security policies and punishes employees who violate cyber security policies. Employees who violate relevant laws and regulations will also bear legal liabilities according to law. ●Financial situation: HUAWEI CLOUD is Huawei's cloud service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue

			has maintained a strong growth trend.
18	When deciding to outsource and select a service provider, financial institutions should consider the possibility of changing service providers and their possible consequences. The service provider must offer a guarantee of permanent service provision.	Customers should consider the professional capabilities of the service provider in its due diligence to ensure that it is able to provide service to the customer on a long-term basis.	HUAWEI CLOUD complies with international standards such as ISO27001, ISO20000, and ISO22301 to establish a comprehensive information security management system, IT service management system, and business continuity management system, and implements the system requirements in daily operations. In addition, HUAWEI CLOUD regularly conducts risk assessment and management review activities every year to identify problems during system operation, implement rectification, and promote continuous improvement of the management system.
18.1	Financial institutions should be prepared to insource or transfer outsourced functions to another service provider in an orderly manner.	Customers should specify the relevant exit plan in the outsourcing agreement, including obligations to support data migration. When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through **Cloud Data Migration (CDM)** provided by HUAWEI CLOUD, such as migrating to local data center. CDM service enables data migration among multiple types of data sources, such as database s, data warehouses and files, and supports data migration across multiple	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.

		environments, such as data migration to the cloud, data exchange in the cloud, and data migration to on premises data centers.	
19	The duties of financial institutions and service providers should be agreed and clearly defined in the contract.	Customers shall specify the respective responsibilities of customers and service provider in the outsourcing agreement.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. For example, HUAWEI CLOUD has certain security obligations and shall take appropriate measures to protect customer data and shall not access customer data unless necessary. In addition, the customer has certain security obligations and is responsible for security vulnerabilities caused by the way the customer uses the account and service. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.
20	Outsourced functions should be incorporated into the internal control system of the financial institution. Main risks associated with outsourcing should be systematically identified, monitored,	Customers shall undertake ongoing oversight of the service provider to identify and address main risks associated with outsourcing.	Customers' rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with financial institutions based on the actual situation. HUAWEI CLOUD will comply with the requirements specified in the agreement signed with customers, and will

	quantified and controlled. Within the financial institution, a department should be designated to monitor and control the service provider. Financial institutions should continuously monitor and evaluate the services of service providers in order to take the necessary measures in a timely manner.		arrange dedicated personnel to actively cooperate with customers and the regulatory authority/agent designated by the regulatory authority to audit and supervise HUAWEI CLOUD.
21	Financial institutions should ensure that outsourcing agreements with service providers give them the right to issue the necessary instructions and controls.	Customers shall specify in the outsourcing agreement that it has the right to issue the necessary instructions and controls to the service provider.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. HUAWEI CLOUD professional service engineers provide 24/7 service support. Customers can contact the HUAWEI CLOUD support team through work orders, intelligent customer service, self-service, and hotline.

5.2 Security

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
24	Where security-relevant functions are outsourced (particularly in information technology), financial institutions and the service provider must contractually agree security requirements. Financial institutions must monitor compliance with these requirements.	Customers should specify security requirements in the outsourcing agreement and monitor compliance by the service provider.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. For example, the outsourcing agreement can specify the security requirements that HUAWEI CLOUD should comply with. Customers' rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with financial institutions based on the actual situation. HUAWEI CLOUD will comply with the requirements specified in the agreement signed with customers, and will arrange dedicated personnel to actively cooperate with customers and the regulatory authority/agent designated by the regulatory authority to audit and supervise HUAWEI CLOUD.
25	Financial institutions and the service provider must draw up a security framework to ensure that the	Customers should develop a business continuity plan, which is regularly tested and updated	HUAWEI CLOUD has developed a business continuity management system that is consistent with its own business characteristics to provide

	outsourced function can continue to be performed in an emergency. In doing so, the financial institutions must apply the same degree of care and attention as it would if it performed the outsourced function itself.	and coordinated with the service provider.	continuous and effective services to customers and ensure the development of customer business. HUAWEI CLOUD conducts internal business continuity publicity and training every year, including regular emergency drills and tests, to continuously optimize emergency response. If customers need HUAWEI CLOUD's participation in their business continuity plans, HUAWEI CLOUD will actively cooperate.

5.3 Audit and Supervision

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
26	Financial institutions, its audit firm and FINMA must be able to verify the service provider’s compliance with supervisory regulations. They must have the contractual right to inspect and audit all information relating to the outsourced function at any time without restriction.	Customers should provide appropriate access, audit and supervision rights in the outsourcing agreement.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. Customers' rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with financial institutions based on the actual situation. HUAWEI CLOUD will comply with the requirements specified in the agreement signed

			with customers, and will arrange dedicated personnel to actively cooperate with customers and the regulatory authority/agent designated by the regulatory authority to audit and supervise HUAWEI CLOUD. HUAWEI CLOUD has passed multiple international security and privacy protection certifications, including ISO 27001, ISO 27017, ISO 27018, SOC, and CSA STAR, and is audited by a third party every year.
29	If the service provider is not supervised by FINMA, it must enter into a contractual obligation with financial institutions to provide FINMA with all the information and documentation concerning the outsourced functions, which are necessary for FINMA's supervisory activities. If auditing is delegated to the service provider's auditors, their report must be supplied, on request, to FINMA as well as to the internal auditors of financial institutions and audit firm.	Customers should provide appropriate access, audit and supervision rights in the outsourcing agreement.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. Customers' rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with financial institutions based on the actual situation. HUAWEI CLOUD will comply with the requirements specified in the agreement signed with customers, and will arrange dedicated personnel to actively cooperate with customers and the regulatory authority/agent designated by the regulatory authority to audit and supervise

			HUAWEI CLOUD.

5.4 Outsourcing Abroad

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
30	Outsourcing to another country is admissible if financial institutions can expressly guarantee that it, its audit firm and FINMA can assert and enforce their right to inspect and audit information.	Customers should provide appropriate access, audit and supervision rights in the outsourcing agreement.	Customers' rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with financial institutions based on the actual situation. HUAWEI CLOUD will comply with the requirements specified in the agreement signed with customers, and will arrange dedicated personnel to actively cooperate with customers and the regulatory authority/agent designated by the regulatory authority to audit and supervise HUAWEI CLOUD.

5.5 Agreement

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
32	The outsourcing must be based on a written agreement or an agreement in some other format that can be evidenced in text form. The outsourcing agreement should include the name and function of the contracting parties.	Customers should enter into a written outsourcing agreement with the service provider, and the names and functions of the contracting parties shall be specified in the outsourcing agreement.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed

33	Financial institutions must ensure that it is informed about the use or replacement of subcontractors for significant functions at an early stage and has the possibility of terminating the outsourcing. Where subcontractors are used, they must also be bound by the obligations and guarantees on the part of the service provider that are necessary to comply with this circular.	Customers should ensure that the outsourcing agreement specifies the following: a. Inform the customer in advance when using or replacing subcontractors. b. Customers have the right to terminate the outsourcing due to the use or replacement of subcontractors; c. Subcontractors must also be bound by the obligations and guarantees on the part of the service provider that are necessary to comply with this circular.	offline contract templates, which can be customized based on customer requirements.
34	The agreement must include the right of financial institutions to issue necessary instructions, the security requirements agreed between financial institutions and service providers, the obligation of service providers to cooperate with regulatory activities, and the right of financial institutions to conduct audits.	Customers should ensure that the outsourcing agreement specifies the following: a. The agreement with the service provider grants it the necessary rights of instruction and control; b. Security requirements agreed by the parties to the contract; c. The obligation of the service provider to cooperate with the regulation; d. Audit rights of interested parties.	

6 How HUAWEI CLOUD Meets and Assists Customers to Meet Circular 2023/1 Operational Risks and Resilience – Banks

FINMA issued Circular 2023/1 Operational Risk and Resilience - Banks on 7 December 2022. This circular is a comprehensive revision of Circular 2008/21 Operational Risk - Banks, improving regulatory practices related to operational risk management and adding the principle of operational resilience to it. Regulatory areas include overall Operational risk management, ICT risk management, Cyber risk management, Critical data risk management, Business continuity management, Management of risks from cross-border service business, and Concerning ensuring operational resilience.

When financial institutions comply with the above provisions, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following content will summarize the requirements related to cloud service providers in the guide, and explain how HUAWEI CLOUD, as a cloud service provider, helps customers meet these control requirements.

6.1 ICT Risk Management

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
51	Financial institutions should ensure that the development or test environments are separate from the ICT production environment.	Customers shall establish and implement environmental isolation measures to ensure the isolation of production environment and non-production environment.	HUAWEI CLOUD has established a formal environment isolation mechanism to logically isolate the development, test, and production environments, improving self-protection and fault tolerance capabilities against external intrusions and internal violations, and reducing risks of unauthorized access or change to the operating environment. Unauthorized network connection between the test environment and production environment is prohibited to prevent

			security risks in the production environment caused by intrusion of the test environment. In addition, HUAWEI CLOUD complies with the principles of separation of duties (SOD) and rights checks and balances, and separates incompatible responsibilities to ensure the separation of responsibilities between development and O&M personnel.
56	Financial institutions shall ensure that it can transition smoothly to its BCP and DRP processes in the event of significant disruptions to its ICT operations. It shall implement adequate back-up processes and recovery processes that are tested and validated regularly.	Customers should develop a business continuity plan and regularly test and update the plan. Customers can back up data through HUAWEI CLOUD's **Cloud Backup and Recovery (CBR)** service to ensure that data will not be lost in the event of a disaster.	HUAWEI CLOUD complies with the ISO22301 international standard for business continuity management and establishes a complete business continuity management system. Under the framework of the system, business impact analysis and risk assessment are performed regularly. HUAWEI CLOUD formulates comprehensive recovery policies for key services that support continuous running of cloud services based on the requirements of the internal business continuity management system. Recovery policies cover all aspects of alternate sites, equipment, personnel, information systems, and third parties, and regularly test the backup and recovery procedures.

57	Financial institutions shall have procedures, processes and controls in place to ensure that ICT that its nearing the end of its operational life or whose planned decommissioning date has passed is dealt with in a risk-oriented way.	Customers should take appropriate measures to properly dispose of the ICT assets that are to be retired.	If customers want to delete data or data needs to be deleted due to the expiration of a service, HUAWEI CLOUD will strictly follow applicable laws and regulations, as well as agreements with customers, delete the stored customer data in accordance with data destruction standards. Data destruction and accidental deletion may lead to data unrecoverable or data loss. Therefore, it is recommended that customers should back up or migrate the data before destroying it.
58	Financial institutions shall have procedures, processes and controls in place for dealing with significant ICT incidents, including those resulting from dependencies on external service providers and outsourcing operations within the group.	Customers should establish and implement event and problem management processes to monitor and record operational and security events, and timely restore key business functions and processes in the event of disruption. **CLOUD Eye Service (CES)** provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take	In line with customer compliance requirements, HUAWEI CLOUD has developed a sound incident management process. This process clearly defines the roles and responsibilities for each activity during the incident management process. The priority of events is divided and defined according to the response time and solution time for each priority of event, which is defined according to the degree of impact and scope. After an incident, HUAWEI CLOUD will decide whether to notify customers of the incident based on the extent of the impact it has on or will have on the customer's business. The contents of the notice include, but are not limited to, descriptions of the incident, causes, impacts, actions taken

		corresponding measures.	by HUAWEI CLOUD, and measures recommended to customers. HUAWEI CLOUD uses the event platform (CIM) to record and track events, starting from event discovery and ending at event closure. Regular trend analysis of events history and identification of similar events help to find and resolve issues. HUAWEI CLOUD deployed a full network alarm system to continuously monitor the utilization of network equipment resources, covering all network equipment. When resource utilization reaches a preset threshold, the alarm system will issue a warning. O&M personnel will take prompt measures to ensure the continuous operation of customer cloud services to the greatest extent. HUAWEI CLOUD has a 24/7 professional security incident response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and communicated according to their real-time status. Moreover, HUAWEI CLOUD will regularly conduct

			statistical and trend analysis of events, and the problem-solving team will find out the root causes of similar incidents and develop solutions to eliminate such incidents from the source.
59	Dealing with significant ICT incidents must be coordinated and linked with the processes for BCM and the DRP.	Customers should establish processes for significant ICT incidents and ensure that they are coordinated with the processes for BCM and the DRP.	HUAWEI CLOUD has also developed a business continuity management system that is consistent with its own business characteristics to provide continuous and effective services to customers and ensure the development of customer business. HUAWEI CLOUD conducts internal business continuity publicity and training every year, including regular emergency drills and tests, to continuously optimize emergency response. If customers need HUAWEI CLOUD's participation in their business continuity plans, HUAWEI CLOUD will actively cooperate.
60	ICT incidents that are regarded by financial institutions as a significant disruption in the provision of its critical processes and are of material significance for supervision must be reported to FINMA without delay.	Customers should establish and implement event and problem management processes and report significant security incidents to FINMA without delay. **CLOUD Eye Service (CES)** provides users with a three-dimensional monitoring	In line with customer compliance requirements, HUAWEI CLOUD has developed a sound incident management process. This process clearly defines the roles and responsibilities for each activity during the incident management process. The priority of events is divided and defined according to the response time and solution time for each

		platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take corresponding measures.	priority of event, which is defined according to the degree of impact and scope. After an incident, HUAWEI CLOUD will decide whether to notify customers of the incident based on the extent of the impact it has on or will have on the customer's business. The contents of the notice include, but are not limited to, descriptions of the incident, causes, impacts, actions taken by HUAWEI CLOUD, and measures recommended to customers. HUAWEI CLOUD uses the event platform (CIM) to record and track events, starting from event discovery and ending at event closure. Regular trend analysis of events history and identification of similar events help to find and resolve issues. HUAWEI CLOUD deployed a full network alarm system to continuously monitor the utilization of network equipment resources, covering all network equipment. When resource utilization reaches a preset threshold, the alarm system will issue a warning. O&M personnel will take prompt measures to ensure the continuous operation of customer cloud services to the greatest extent. HUAWEI CLOUD has a 24/7 professional security incident

			response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and communicated according to their real-time status. Moreover, HUAWEI CLOUD will regularly conduct statistical and trend analysis of events, and the problem-solving team will find out the root causes of similar incidents and develop solutions to eliminate such incidents from the source.

6.2 Cyber Risk Management

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
62	Financial institutions shall define clear tasks, competencies and responsibilities. It must cover at least the following aspects: a. Identification of the financial institution-specific threat landscape from cyber attacks and assessment of the possible impacts of exploiting vulnerabilities with regard to the	Customers should take appropriate measures to ensure the security of their ICT assets.	HUAWEI CLOUD attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. HUAWEI CLOUD will continue to embrace industry leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects,

	inventoried ICT assets and the electronic critical data b. Protection of the inventoried ICT assets and the electronic critical data from cyber attacks by implementing appropriate protective measures, particularly with regard to the confidentiality, integrity and availability; c. Timely logging and detection of cyber attacks on the basis of a process for the systematic and consistent monitoring of the inventoried ICT assets and the electronic critical data; d. Response to identified vulnerabilities and cyber attacks by developing and implementing appropriate processes for taking rapid containment and remediation measures; and e. Ensuring the prompt recovery of normal business operations after a cyber attack through appropriate measures.		including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, HUAWEI CLOUD will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business. HUAWEI CLOUD explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the laws and regulations or the binding orders of the government institutions. And at the same time, it will clearly stipulate the responsibility of HUAWEI CLOUD to customers in the case of a breach of confidentiality clauses in contracts signed with customers in the financial industry. In addition, HUAWEI CLOUD service products and components have planned and implemented isolation mechanism from the beginning of design, avoiding unauthorized access and tampering between customers intentionally or unintentionally, and reducing the risk of data leakage. Using data

			storage as an example, HUAWEI CLOUD services including block storage, object storage, and file storage all regard customer data isolation as an important feature. In line with customer compliance requirements, HUAWEI CLOUD has developed a sound incident management process. This process clearly defines the roles and responsibilities for each activity during the incident management process. The priority of events is divided and defined according to the response time and solution time for each priority of event, which is defined according to the degree of impact and scope. HUAWEI CLOUD uses the event platform (CIM) to record and track events, starting from event discovery and ending at event closure. Regular trend analysis of events history and identification of similar events help to find and resolve issues. HUAWEI CLOUD has a 24/7 professional security incident response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and

			communicated according to their real-time status. Moreover, HUAWEI CLOUD will regularly conduct statistical and trend analysis of events, and the problem-solving team will find out the root causes of similar incidents and develop solutions to eliminate such incidents from the source. HUAWEI CLOUD CSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and exposure. Additionally, HUAWEI CLOUD will actively implement quality assurance of cloud product and platform security, and conducts internal and third-party penetration testing and security assessments each year to ensure the HUAWEI CLOUD environment is secure. HUAWEI CLOUD security exercise team regularly develops exercises for different product types (including basic services, operation centers, data centers, and overall organization, etc.) and different scenarios to maintain the effectiveness of the continuous plan. When significant changes take place in the organization and environment of HUAWEI CLOUD, the effectiveness of business

			continuity level would also be tested. HUAWEI CLOUD has formulated various specific contingency plans which specifies the organization, procedures, and operation specifications for emergency response to deal with complex security risks in the cloud environment. Each year, HUAWEI CLOUD conducts contingency plan drills for major security risk scenarios to quickly reduce potential security risks and ensure continuous running of cloud services and ensure customer service and data security.
68	Financial institutions should conduct a preliminary assessment of cyber attacks within 24 hours and notify FINMA when the preliminary assessment is completed. Financial institutions should submit to FINMA, within 72 hours, a detailed report that meets the requirements. Financial institutions should submit to FINMA a root cause analysis that is consistent with the severity of the cyber attack after completing the handling of a cyber attack.	Customers should complete the assessment of cyber attacks within the specified time and submit the risk assessment report and root cause analysis report to FINMA.	In line with customer compliance requirements, HUAWEI CLOUD has developed a sound incident management process. This process clearly defines the roles and responsibilities for each activity during the incident management process. The priority of events is divided and defined according to the response time and solution time for each priority of event, which is defined according to the degree of impact and scope. After an incident, HUAWEI CLOUD will decide whether to notify customers of the incident based on the extent of the impact it has on or will have on the customer's business. The contents of the notice include, but are not limited to,

			descriptions of the incident, causes, impacts, actions taken by HUAWEI CLOUD, and measures recommended to customers. HUAWEI CLOUD uses the event platform (CIM) to record and track events, starting from event discovery and ending at event closure. Regular trend analysis of events history and identification of similar events help to find and resolve issues.
69	Financial institutions should regularly arrange for professionals to conduct vulnerability assessments and penetration tests on all inventoried ICT assets.	Customers should test ICT systems, services and information security measures to identify potential security weaknesses and violations. Such as code review, penetration testing, vulnerability scanning, etc.	HUAWEI CLOUD CSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and exposure. Additionally, HUAWEI CLOUD will actively implement quality assurance of cloud product and platform security, and conducts internal and third-party penetration testing and security assessments each year to ensure the HUAWEI CLOUD environment is secure.
70	Risk-based, threat intelligence-related scenario cyber exercises must be conducted on the basis of the financial institution-specific threat landscape. The result of the exercises must be documented and reported in an appropriate form.	Customers should regularly conduct cyber security exercises. The result of the exercises must be documented and reported in an appropriate form.	HUAWEI CLOUD regularly conducts internal practical cybersecurity field exercises (red team and blue team exercises,) and third-party penetration testing and security assessment with regular monitoring, checks, and removal of any security threats so as to guarantee the security of the cloud services.

6.3 Critical Data Risk Management

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
76	Critical data must be adequately protected from being accessed and used by unauthorised persons.	Customers should implement data security measures to protect data from being erased, destroyed, accidentally destroyed, modified and damaged, and unauthorized access. To prevent this data from being downloaded wrongfully, customers can use different ways to audit and detect abnormal activities for different products and services. For example, for object storage, file storage and other services, customers can use **Cloud Trace Service (CTS)** to record user operations on data. For relational database services, customers can use database security services for column-level database management, and can access activity records.	HUAWEI CLOUD attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. HUAWEI CLOUD will continue to embrace industry leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, HUAWEI CLOUD will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business. HUAWEI CLOUD explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the laws and regulations or the binding orders of the government institutions. And at the same time, it will clearly stipulate the responsibility of HUAWEI CLOUD to customers in the case of a breach of confidentiality clauses in contracts signed with customers in the financial

			industry. In addition, HUAWEI CLOUD service products and components have planned and implemented isolation mechanism from the beginning of design, avoiding unauthorized access and tampering between customers intentionally or unintentionally, and reducing the risk of data leakage. Using data storage as an example, HUAWEI CLOUD services including block storage, object storage, and file storage all regard customer data isolation as an important feature.
77	The ICT assets that store or process critical data must be afforded particular protection. Access to these data must be regulated systematically and monitored continuously.	Customers should monitor for unusual activity through logs and periodically review and analyze them. HUAWEI CLOUD's **Cloud Trace Service (CTS)** provides collection, storage, and querying of operational records for a variety of cloud resources to support common scenarios such as security analysis, compliance auditing, resource tracking, and problem location. **Log Tank Service (LTS)** provided by HUAWEI CLOUD collects, queries, and stores logs in real time. It records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing.	HUAWEI CLOUD has a centralized and complete log big data analysis system. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components in a unified manner to support cyber security event backtracking and compliance. The log analysis system has powerful data storage and query capabilities, ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days.

		Combining with Cloud Eye, Customers can monitor user login logs in real time. When malicious logins occur, an alarm is generated and requests from the IP address are rejected.	
78	Access to critical data and processing functionalities shall be restricted to persons who require this to carry out their tasks. Financial institutions must have an authorisation system in place. Access to this authorisation system must be afforded particular protection and reviewed on a regular basis. The authorisations included in the authorisation system must be reviewed on a regular basis.	Customers should ensure that access to data and systems follows the "principle of minimum authority". HUAWEI CLOUD provides **Identity and Access Management (IAM)** for customers to manage their accounts that use cloud resources. Customers can use IAM to perform role-based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system, for example, setting an access control list (ACL), to prevent malicious access from untrusted networks. Customers should establish a user access management	HUAWEI CLOUD implements role-based access control and permission management for internal personnel, restricting personnel with different positions and responsibilities to only perform specific operations on authorized targets. Ensure that personnel do not gain unauthorized access through minimal privilege assignment and strict behavioral auditing. HUAWEI CLOUD has specified the maximum review period for accounts/ rights at different levels. The account/right owner periodically reviews the accounts/rights held by the account/right owner and submits a deregistration application when the user is transferred or the role changed.

		mechanism to restrict and supervise the access to the system based on the least privilege principle.	
79	If critical data is stored outside of Switzerland or if it can be accessed from abroad, increased risks associated with this must be adequately mitigated and monitored via suitable means and the data afforded particular protection.	Customers should take appropriate security measures to protect critical data and continuously monitor and mitigate risks. Customers can use multiple privacy protection technologies and services provided by HUAWEI CLOUD, including **Identity and Access Management (IAM)**, **Data Encryption Workshop (DEW)**, and **Log Tank Service (LTS)** and **Cloud Trace Service (CTS)** provide users with functions such as access control and identity authentication, data encryption, logging, and auditing, helping users protect personal data based on service requirements.	HUAWEI CLOUD explicitly states in the user agreement that it will not access or use the user's content, unless it provides the necessary services for the user or abides by the laws and regulations or the binding orders of the government institutions. And at the same time, it will clearly stipulate the responsibility of HUAWEI CLOUD to customers in the case of a breach of confidentiality clauses in contracts signed with customers in the financial industry. HUAWEI CLOUD strictly abides by all applicable laws and regulations concerning data security and privacy protection. In terms of cross-border data transfer, HUAWEI CLOUD provides customers with interfaces for signing and querying privacy notices, and notifies data subjects of possible data transfer outside Europe. Customers can select the server area where content data is stored as required. Without the customer's consent, HUAWEI CLOUD will not migrate the customer's content data from the selected server area. HUAWEI CLOUD service products and components have planned and implemented isolation mechanism from the beginning of design, avoiding unauthorized access and tampering between customers intentionally or unintentionally, and reducing the risk of data leakage. Using data storage as an example,

			HUAWEI CLOUD services including block storage, object storage, and file storage all regard customer data isolation as an important feature. HUAWEI CLOUD has obtained multiple international security and privacy protection certifications, including ISO 27001, ISO 27017, ISO 27018, SOC, and CSA STAR. HUAWEI CLOUD has obtained multiple international authoritative security and privacy protection certifications. Third-party assessment companies will also regularly conduct confidentiality, security adequacy, and compliance audits on HUAWEI CLOUD and issue third-party audit reports. Requirements for obtaining third-party audit reports can be specified in the agreement signed by the customer based on the actual situation. To help customers meet compliance requirements, HUAWEI CLOUD has established a comprehensive information security and privacy protection management system based on various laws and regulations, regulatory requirements, and international or industry standards, and continuously improved it. In addition, HUAWEI CLOUD regularly conducts internal and third-party penetration tests and security assessments to monitor, identify, and resolve security threats and ensure the security of cloud services.
80	Both internal and external persons who can access critical data or who can change these must be selected carefully. These persons must be monitored with the	Customers should develop and implement a security awareness training plan, implement a dedicated personnel	To improve the cyber security awareness of all employees, avoid cyber security violation risks, and ensure normal business operations, HUAWEI CLOUD has carried out security awareness education in three aspects: popularize

	help of appropriate measures and given regular training in the handling of these data. In addition, a list of all persons with privileged access rights must be kept and updated on a regular basis.	management plan for key positions, and regularly train them on IT security behavior.	awareness education, carry out publicity activities, and sign the business conduct code and commitment letter for employees. In addition, a special information security awareness training plan is developed, and security awareness training for all employees is conducted at least once a year. Awareness education includes but is not limited to on-site lectures and video online courses. In addition, to manage personnel in an orderly manner and reduce the potential impact of personnel management risks on business continuity and security, HUAWEI CLOUD implements a dedicated personnel management plan for key positions such as O&M engineers, including onboarding security review, on-the-job security training and enablement, onboarding qualification management, and exit security review.
81	Incidents that substantially impair the confidentiality, integrity or availability of critical data must be reported to FINMA without delay.	Customers establish and implement incident and problem management processes to report significant security incidents to regulators in a timely manner.	In line with customer compliance requirements, HUAWEI CLOUD has developed a sound incident management process. This process clearly defines the roles and responsibilities for each activity during the incident management process. The priority of events is divided and defined according to the response time and solution time for each priority of event, which is defined according to the degree of impact and scope. After an incident, HUAWEI CLOUD will decide whether to notify customers of the incident based on the extent of the impact it has on or will have on the customer's business. The contents of the notice include, but are not limited to,

			descriptions of the incident, causes, impacts, actions taken by HUAWEI CLOUD, and measures recommended to customers. HUAWEI CLOUD uses the event platform (CIM) to record and track events, starting from event discovery and ending at event closure. Regular trend analysis of events history and identification of similar events help to find and resolve issues. HUAWEI CLOUD deployed a full network alarm system to continuously monitor the utilization of network equipment resources, covering all network equipment. When resource utilization reaches a preset threshold, the alarm system will issue a warning. O&M personnel will take prompt measures to ensure the continuous operation of customer cloud services to the greatest extent. HUAWEI CLOUD has a 24/7 professional security incident response team responsible for real-time monitoring and notification. The team follows standard criteria for response and resolution time, and can quickly detect, demarcate, isolate, and recover from major events. Events are escalated and communicated according to their real-time status. Moreover, HUAWEI CLOUD will regularly conduct statistical and trend analysis of events, and the problem-solving team will find out the root causes of similar incidents and develop solutions to eliminate such incidents from the source.
82	When selecting service providers that can process or view critical data, due diligence must be particularly thorough.	Customers should conduct due diligence on service providers that can process or access critical data	Customers' rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with financial institutions based on the actual situation. HUAWEI

	Clear criteria for assessing how service providers handle critical data must be defined and checked before entering into a contractual agreement. The service providers must be monitored and checked periodically as part of the financial institution's internal control system.	to understand their standards for handling critical data, and should monitor and regularly check implementation.	CLOUD will comply with the requirements specified in the agreement signed with customers, and will arrange dedicated personnel to actively cooperate with customers and the regulatory authority/agent designated by the regulatory authority to audit and supervise HUAWEI CLOUD.

6.4 Business Continuity Management

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
85	Financial institutions shall define the RTO and RPO for the critical processes. These shall be coordinated with the necessary service providers and adherence to the RTO and RPO shall be regulated by service level agreements or contracts or by other appropriate procedures, processes and controls.	Customers should perform business impact analysis, identify critical processes, and determine the RTO and RPO of critical processes. At the same time, customers should specify the relevant content in the outsourcing agreement and standardize the compliance of the service provider.	HUAWEI CLOUD has established a comprehensive business continuity management system in compliance with the ISO22301 international standard for business continuity management. Based on the requirements of the system framework, HUAWEI CLOUD periodically analyzes service impact, identifies key services, and determines the recovery objectives and minimum recovery level of key services. In the process of identifying key services, the impact of service interruption on customers is an important criterion for judging key services. If customers need HUAWEI CLOUD's participation in their business continuity plans, HUAWEI CLOUD will actively cooperate.
87	The BIA and BCP shall be prepared and documented in a consistent manner following institution-wide guidelines. They	Customers should develop a business continuity plan that is regularly tested and updated to maintain the	HUAWEI CLOUD has rich business continuity management and disaster recovery policies and processes. The Business Continuity Plan is developed

	must be reviewed and updated annually and on an ad hoc basis in the event of significant changes to the business operations.	effectiveness of the recovery strategy.	and reviewed annually by the Business Continuity Management Team and is updated based on the results of the review. The Business Continuity Management team performs a business impact analysis and risk assessment annually, including the identification of critical business processes, maximum tolerable downtime, recovery time objectives, minimum service levels, and time required to restore service. The report identifies and records threats that may interrupt HUAWEI CLOUD services and resources, and designs policies for different service interruption scenarios of HUAWEI CLOUD products. The results of the business impact analysis and risk assessment are documented in the risk assessment report. According to the plan, HUAWEI CLOUD conducts business continuity drills and tests on all products within the scope at least every year. Record and review the results of business continuity drill tests.
90	Financial institutions shall define a communication strategy for internal and external communication in crisis situations.	Customers should develop and implement a crisis communication strategy.	HUAWEI CLOUD, as a service provider of an authorized institution, will actively cooperate with the authorized institution to proactively initiate communication. HUAWEI CLOUD professional service engineers provide 24/7 service support. Customers can contact the HUAWEI CLOUD support team through work orders, intelligent customer service, self-service, and hotline. In addition, HUAWEI CLOUD has developed crisis communication policies based on the requirements of the internal business continuity management system, defining the communication objects,

			communication contents, and communication tools in case of emergencies.
91	The implementation of the BCP and DRP as well as the functioning of the crisis organisation must be regularly evaluated through tests. Systematic plans shall be drawn up for this, which ensure regular coverage.	Customers should develop a business continuity plan and disaster recovery plan and regularly test it to maintain the effectiveness of the recovery strategy.	HUAWEI CLOUD has developed a disaster recovery plan and periodically tests it. For example, the cloud platform infrastructure and cloud services in a geographical location or region are offline, a disaster is simulated, and the system is processed and transferred according to the disaster recovery plan to verify the business and operational functions of the fault location. The test results are annotated and archived to continuously improve the plan. HUAWEI CLOUD has rich business continuity management and disaster recovery policies and processes. The Business Continuity Plan is developed and reviewed annually by the Business Continuity Management Team and is updated based on the results of the review. The Business Continuity Management team performs a business impact analysis and risk assessment annually, including the identification of critical business processes, maximum tolerable downtime, recovery time objectives, minimum service levels, and time required to restore service. The report identifies and records threats that may interrupt HUAWEI CLOUD services and resources, and designs policies for different service interruption scenarios of HUAWEI CLOUD products. The results of the business impact analysis and risk assessment are documented in the risk assessment report. According to the plan, HUAWEI CLOUD conducts business continuity drills and

			tests on all products within the scope at least every year. Record and review the results of business continuity drill tests.
96	The employees and members of the crisis organisation shall be adequately trained in their tasks, competencies and responsibilities resulting from the various BCM activities, both when new employees join the financial institution and as part of regular training.	Customers should regularly train relevant employees on business continuity.	HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics to continuously and effectively provide services for customers and ensure their business development. HUAWEI CLOUD conducts business continuity publicity and training in the organization every year, provides special training for employees in crisis management positions, and regularly conducts emergency drills and tests to continuously optimize the emergency response mechanism.

7 How HUAWEI CLOUD Meets and Assists Customers to Meet Cloud Guidelines

SBA released the Cloud Guidelines on June 1, 2020, identifying four key areas related to the delivery of banking and financial services through cloud technologies, including governance, data and data security, authorities and proceedings, and audit of cloud services and means used. The guide provides recommendations on how to manage these areas. These recommendations are not legally binding. Banks can apply this guidance as a best practice given their size and complexity of their business model.

When financial institutions comply with the above provisions, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following content will summarize the requirements related to cloud service providers in the guide, and explain how HUAWEI CLOUD, as a cloud service provider, helps customers meet these control requirements.

7.1 Responsibilities and Roles

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
10	When allocating responsibilities and defining roles, the service and delivery models must be considered. The service provider should cooperate as appropriate and necessary, making relevant information available to the financial institution.	Customers should ensure that the roles of customers, the service provider and the relevant parties are clearly defined in the outsourcing agreement.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. For example, HUAWEI CLOUD has certain security obligations and shall take appropriate measures to protect customer data and shall not access customer data unless necessary. In addition, the customer has certain security obligations and is responsible for security vulnerabilities caused by the way the
12	The contract between the financial institution and the service provider should set out the corresponding rights and duties of the parties and others involved, and should	Customers should clearly define the responsibilities of the parties involved in the outsourcing agreement.	

	also cover their implementation.		customer uses the account and service. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.

7.2 Selecting and Changing the Provider and Significant Subcontractors

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
14	When selecting the appropriate service provider, it is in the financial institution's interest to take account of the service provider's ability to fulfil the contractual obligations, its financial stability and the jurisdiction to which it is subject, as well as other essential points. Significant subcontractors should be included in the assessment. The service provider should assist as appropriate in gathering the information on this matter requested by the financial institution.	When selecting a service provider, customers should consider its professional capabilities, financial situation and the management of the supplier in due diligence.	HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements and due diligence initiated by the customer. HUAWEI CLOUD has passed multiple international security and privacy protection certifications, including ISO 27001, ISO 27017, ISO 27018, SOC, and CSA STAR, and is audited by a third party every year. ●Professional capabilities: HUAWEI CLOUD complies with international standards such as ISO27001, ISO20000, and ISO22301 to establish a comprehensive information security management system, IT service management system, and business continuity management system, and implements the system requirements in daily operations. In addition, HUAWEI CLOUD regularly conducts risk assessment and management review

			activities every year to identify problems during system operation, implement rectification, and promote continuous improvement of the management system. ●Financial situation: HUAWEI CLOUD is Huawei's cloud service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue has maintained a strong growth trend. ●Supplier management: HUAWEI CLOUD has developed its own supplier management mechanism, which raises security requirements for both suppliers' products and internal management. In addition, HUAWEI CLOUD regularly audits suppliers and audits risky suppliers on site. HUAWEI CLOUD will also sign cyber security agreements with suppliers involved in cyber security. During the service process, HUAWEI CLOUD will continuously monitor their service quality, score suppliers' performance, and degrade suppliers with poor security performance.
16	When selecting a service provider, its willingness to assume responsibility for the essential duties arising out of financial market and data protection legislation and the design of its operating model should be considered in	Customers should consider the performance, compliance and information security management of the service provider in its due diligence.	HUAWEI CLOUD will assign dedicated personnel to actively cooperate with the audit requirements and due diligence initiated by the customer. HUAWEI CLOUD has passed multiple international security and privacy protection certifications, including ISO 27001, ISO 27017, ISO 27018, SOC, and CSA STAR, and is

	addition to performance-related criteria. When selecting a service provider and its subcontractors to process CID from the financial institution or other personal data, the confidentiality and security of the data should be a decisive criterion and an integral part of the underlying due diligence.		audited by a third party every year. ●Performance: HUAWEI CLOUD is Huawei's cloud service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue has maintained a strong growth trend. ●Compliance: For regions that provide cloud services, HUAWEI CLOUD actively communicates with regulators to understand their concerns and requirements, contributes HUAWEI CLOUD knowledge and experience, and continuously consolidates HUAWEI CLOUD's compliance with relevant laws and regulations in terms of cloud technologies, cloud services, and cloud security. In addition, HUAWEI CLOUD shares the analysis results of laws and regulations with tenants to avoid violation risks caused by information loss. The security responsibilities of both parties are specified in contracts. On one hand, HUAWEI CLOUD meets regulatory requirements through cross-industry and cross-region cloud security certifications. On the other hand, HUAWEI CLOUD builds and consolidates customer trust in HUAWEI CLOUD services by obtaining

			security certifications required by key industries and regions. Finally, a secure cloud environment is built among law and regulation makers, administrators, and tenants. ●Information security management: HUAWEI CLOUD builds a comprehensive information security management system based on ISO27001 and formulates an overall information security policy for HUAWEI CLOUD. The policy specifies the architecture and responsibilities of the information security management organization, management methods of information security system documents, and key directions and objectives of information security, including: Asset security, access control, cryptography, physical security, operation security, communication security, system development security, supplier management, information security event management, and business continuity ensure the confidentiality, integrity, and availability of customer systems and data. In addition, HUAWEI CLOUD focuses on the security awareness development of employees and outsourcing personnel, and formulates and regularly implements the

			security awareness training plan.
17	A change of service provider should be subject to the prior consent of the financial institution, which may be given in writing or another verifiable manner. A restructuring that is purely internal to the group and within the same jurisdiction that does not have a material impact on the existing circumstances, criteria and risks may be exempted from this consent requirement. The service provider should, at the financial institution's request, agree to put in place arrangements governing a change of financial institutions controlling the service provider or a significant subcontractor.	Customers shall specify in the outsourcing agreement that the service provider shall obtain the prior consent of customers to change the service provider.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.
18	In any event the financial institutions must be notified before the service provider involves a new significant subcontractor and given the opportunity to terminate the contract with the service provider, while appropriate measures are taken to transfer the outsourced functions in an orderly manner.	Customers should ensure that the outsourcing agreement includes the following: a. Service provider shall inform customers in advance of the change of new significant subcontractors; b. Customers have the right to terminate the outsourcing due to the change of significant subcontractors; c. Exit policy terms, including obligations to support data migration.	

		When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through **Cloud Data Migration (CDM)** provided by HUAWEI CLOUD, such as migrating to local data center. CDM service enables data migration among multiple types of data sources, such as database s, data warehouses and files, and supports data migration across multiple environments, such as data migration to the cloud, data exchange in the cloud, and data migration to on premises data centers.	

7.3 Data Centres and Operating Centres

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
20	The service provider should disclose the locations where the cloud infrastructures (data centres) that the financial institution deploys (or can deploy) are situated and from which the cloud is operated (operating centres), as well as changes of location during the period of deployment. This disclosure should include information on the (legal) entities, specifically the service provider and significant subcontractors, that operate, own or otherwise control the data	Service provider shall disclose to customers information such as the location of the data centres and operating centres.	HUAWEI CLOUD provides an online **Data Processing Addendum**, which clearly discloses the location of the data center that can be deployed by the customer (Currently, the data center of HUAWEI CLOUD Europe is deployed in Ireland. The location of the data center in Europe will be updated from time to time.) and other related information.

	centres and operating centres.		If the location of the data center and operation center changes during the customer's deployment, HUAWEI CLOUD will update related information in a timely manner. In addition, HUAWEI CLOUD will disclose relevant information to customers based on their requirements, such as information about important subcontractors.
21	Where protected information is involved, a change of location to another jurisdiction during the term of the contract should be subject to a contractually defined change procedure and, depending on the individual need for protection, require the prior consent of the financial institution. The service provider should detail the risks associated with the change of location and supply the financial institution with all the relevant information, in particular regarding the security measures applied, to enable it to take a decision.	Where protected information is involved, customers should ensure that the outsourcing agreement includes the following: a. Change procedures; b. Change the location of the data centres and operating centres with the prior consent of customers (depending on the customer's need). Service provider shall provide the customers with information to fully understand the risks associated with changing the location. If customers have data migration requirements, they can use the **Cloud Data Migration (CDM)** of	HUAWEI CLOUD provides services for customers by region. Regions are the storage locations of customers' content data. HUAWEI CLOUD will never move customers' content data across regions without users' authorization. When using cloud services, you are advised to select a region based on the nearby access principle and laws and regulations of different regions to ensure that content data is stored in the target location. HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by

		HUAWEI CLOUD.	HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. HUAWEI CLOUD, as a service provider of an authorized institution, will actively cooperate with the authorized institution to proactively initiate communication and provide corresponding materials.
22	Financial institutions have the right to refuse prior consent without reason. The financial institutions have the right to terminate the outsourcing due to a change of location and to take appropriate measures to transfer the outsourced functions in an orderly manner.	Customers should ensure that the outsourcing agreement includes the following: a. Customers have the right to terminate the outsourcing due to the location change of the data centres and operating centres; b. Exit policy terms, including supporting data migration obligations. When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through **Cloud Data Migration (CDM)**	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements.

		provided by HUAWEI CLOUD, such as migrating to local data center. CDM service enables data migration among multiple types of data sources, such as database s, data warehouses and files, and supports data migration across multiple environments, such as data migration to the cloud, data exchange in the cloud, and data migration to on premises data centers.	

7.4 Storage Locations and Data Flows, Access Concept

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
27	The service provider should allow the financial institution to review the acceptability of the locations where the CID and, where relevant, other protected information are processed and inspect those locations. Financial institutions should also be in a position to comply with its duties of transparency to clients and therefore know where processing is	Customers shall have the right to know where the service provider stores the data and to disclose that location information to its customers.	HUAWEI CLOUD has provided cloud services in multiple countries or regions around the world. Its infrastructure is deployed in multiple regions and availability zones (AZs) around the world. With this deployment mode, HUAWEI CLOUD can flexibly replace computing and storage instance resources in multiple geographical regions or among AZs in the same region. Each AZ is an independent fault maintenance domain. That is, AZs are physically isolated. Users can make full use

	carried out (in particular the locations where protected information is stored) to the level of detail required for this purpose.		of these geographic regions and AZs to plan, deploy, and run application systems on the cloud. Distributed deployment of applications based on multiple AZs ensures that application systems can run continuously in the case of most faults. For more information about HUAWEI CLOUD infrastructure, see Global Infrastructure on the HUAWEI CLOUD official website. HUAWEI CLOUD provides services for customers by region. Regions are the storage locations of customers' content data. HUAWEI CLOUD will never move customers' content data across regions without users' authorization. When using cloud services, you are advised to select a region based on the nearby access principle and laws and regulations of different regions to ensure that content data is stored in the target location. For regional services, customers can select regions as required at the initial stage of service purchase. The service deployment location and data storage location can be changed on the HUAWEI CLOUD portal.
28	Data flows involving protected information, which take place in the sphere of the service provider and, where relevant, its	Where transmission of protected information is involved between service providers and related subcontractors, customers shall	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service

	subcontractors, should be disclosed to the financial institution in advance and the architecture underlying the data flows should, where required, be specified as precisely as necessary in the contract.	ensure the structure of the data flow that includes protected information in the outsourcing agreement, in accordance with its own needs.	content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. If required by the customer, HUAWEI CLOUD will disclose information about subcontractors and data flows in the data processing agreement signed with the customer.
29	Service provider should disclose access authorisations granted on request and access to protected information, in particular CID, should be monitored and recorded in an appropriate manner by the service provider.	Customers have the right to know authorization to access protected information and to record and monitor access to protected information.	HUAWEI CLOUD implements role-based access control and permission management for internal personnel, restricting personnel with different positions and responsibilities to only perform specific operations on authorized targets. Ensure that personnel do not gain unauthorized access through minimal privilege assignment and strict behavioral auditing. HUAWEI CLOUD has a centralized and complete log big data analysis system. The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components in a unified manner to support cyber security event backtracking and compliance. The log analysis system has

			powerful data storage and query capabilities, ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days.

7.5 General Technical and Organisational Measures on Data Security

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
31	Service provider should offer and, in accordance with the agreement, implement appropriate technical and organisational measures to protect the financial institution's protected information that it is processing. International and local standards should be taken into account. The subcontractors and the members of staff deployed by the service provider and the subcontractors should also, where applicable, be bound to comply with such measures.	Customers shall ensure that appropriate technical and organizational measures are defined in the outsourcing agreement. Employees of the service provider and its subcontractors shall comply with the relevant measures.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, it also includes the security measures implemented by HUAWEI CLOUD. For example, encryption, access control, event management, configuration management, and third-party security audit on HUAWEI CLOUD. HUAWEI CLOUD will continuously update and improve security measures to ensure the security of customer data. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized

			based on customer requirements. HUAWEI CLOUD attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. HUAWEI CLOUD will continue to embrace industry leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, HUAWEI CLOUD will always strive toward the most practical and effective data protection possible in order to best safeguard the privacy, ownership, and control of our tenants' data against data breaches and impacts on their business. HUAWEI CLOUD clearly states in the user agreement that it will not access or use users' content unless it provides necessary services for users, complies with laws and regulations or binding orders of government agencies, and strictly complies with all applicable laws and regulations related to data security and privacy protection. In addition, the contract signed with the customer will specify the responsibilities that

			HUAWEI CLOUD shall bear to the customer in case of violation of the confidentiality clause. In addition, isolation mechanisms are planned and implemented for HUAWEI CLOUD service products and components from the beginning of design to prevent unauthorized access and tampering between customers and reduce data leakage risks. Take data storage as an example. HUAWEI CLOUD block storage, object storage, and file storage services take customer data isolation as an important feature. HUAWEI CLOUD has developed its own supplier management mechanism, which raises security requirements for both suppliers' products and internal management. In addition, HUAWEI CLOUD regularly audits suppliers and audits risky suppliers on site. HUAWEI CLOUD will also sign cyber security agreements with suppliers involved in cyber security. During the service process, HUAWEI CLOUD will continuously monitor their service quality, score suppliers' performance, and degrade suppliers with poor security performance.
32	Service provider should ensure that its staff and those of the subcontractors that have access to protected information,	Service provider and subcontractor employees shall undertake confidentiality commitments and conduct regular	To improve the cyber security awareness of all employees, avoid cyber security violation risks, and ensure normal business operations, HUAWEI CLOUD has carried out security

	including CID, verifiably undertake to maintain confidentiality and treat the data accordingly, and receive information and training to this effect.	training for their employees.	awareness education in three aspects: popularize awareness education, carry out publicity activities, and sign the business conduct code and commitment letter for employees. In addition, a special information security awareness training plan is developed, and security awareness training for all employees is conducted at least once a year. Awareness education includes but is not limited to on-site lectures and video online courses.

7.6 Banking Secrecy and Security Measures

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
33	Financial institutions should take appropriate technical and organizational security measures to maintain the security of customer identification data processed using cloud services. The security measures to be considered by financial institutions are described in Circular No. 2008/21. (The Circular has been fully revised by Circular 2023/1 Operational Risk and Resilience - Banks).	Customers shall take appropriate technical and organizational security measures to maintain the security of the customer identification data processed by the cloud service.	For details, see the internal practices of HUAWEI CLOUD in "6. How HUAWEI CLOUD Meets and Assists Customers to Meet Circular 2023/1 Operational Risks and Resilience – Banks".

7.7 Authorities and Proceedings

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
57	Service provider must agree with the financial institution a procedure for both parties to adopt in response to requests from the authorities relating to the handover or transfer of protected information that is processed in the cloud, and this must be specified in the outsourcing agreement.	Customers should specify in the outsourcing agreement the process for responding to requests from authorities relating to the handover or transfer of protected information that is processed in the cloud.	HUAWEI CLOUD provides the **HUAWEI CLOUD User Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the service content and service level provided by HUAWEI CLOUD, and the responsibilities of HUAWEI CLOUD. In addition, HUAWEI CLOUD has developed offline contract templates, which can be customized based on customer requirements. If required by the customer, HUAWEI CLOUD will disclose information about subcontractors and data flows in the data processing agreement signed with the customer.
58	In the context of foreign proceedings the service provider, its subcontractors and group companies may only transfer or disclose protected information processed in the cloud to foreign authorities or other parties abroad in accordance with the applicable legal and regulatory provisions and (i) with the prior written consent of the financial institution, (ii) on the basis of a judgment of the competent Swiss court, or (iii) on	Customers shall specify in the outsourcing agreement that, In the context of foreign proceedings, the service provider, its subcontractors and the group company may transfer protected information processed in the cloud to foreign authorities or other foreign interested parties only if: a. Clearly defined by legal or regulatory requirements; b. Prior written consent of the financial institution; c. Judgment of a competent Switzerland court;	

	the basis of an authorisation from the competent Swiss authority.	d. Switzerland Authorisation by the competent authority.	
59	Service provider should notify the financial institution in due time prior to handing over the protected information, give the financial institution the rights to conduct the proceedings, and support the financial institution in handling requests from foreign authorities.	Customers shall specify in the outsourcing agreement that the service provider shall notify the financial institution in a timely manner prior to the transfer of the protected information.	
60	If, on account of mandatory law, the service provider is unable to notify the financial institution in advance of the transfer or disclosure of protected information to foreign authorities or other parties abroad, the service provider should implement the appropriate legal or protective measures within the scope of the agreement made and in the interest of the financial institution and its clients.	Customers shall specify in the outsourcing agreement that if the service provider is unable to notify the financial institution prior to transferring the protected information to a foreign authority or other foreign interested party due to mandatory legal requirements, the service provider shall implement appropriate legal or protective measures within the scope of the contract.	

7.8 Audit of the Cloud Services and Means Used

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
64	Compliance with the requirements applicable to or contractually imposed on the service provider arising out of the legal and regulatory requirements should be audited regularly. The service provider should assist in this process to an appropriate extent. Performance of the contractually agreed services may also form part of the audit.	Customers shall provide appropriate access, audit and oversight rights in the outsourcing agreement.	Customers' rights to audit and monitor HUAWEI CLOUD will be committed in the agreement signed with financial institutions based on the actual situation. HUAWEI CLOUD will comply with the requirements specified in the agreement signed with customers, and will arrange dedicated personnel to actively cooperate with customers and the regulatory authority/agent designated by the regulatory authority to audit and supervise HUAWEI CLOUD.

8 How HUAWEI CLOUD Meets and Assists Customers to Meet Guidance 05/2020

FINMA published Guidance 05/2020 on May 7, 2020. There is a requirement for all FINMA-supervised institutions to report to regulators in the event of a material cyberattack, and details of reporting obligations are specified.

When financial institutions comply with the above provisions, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following content will summarize the requirements related to cloud service providers in the guide, and explain how HUAWEI CLOUD, as a cloud service provider, helps customers meet these control requirements.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
3	1. Immediate reporting to FINMA means that the affected supervised institution informs FINMA through the responsible (Key) Account Manager within 24 hours of detecting such a cyber attack and conducting an initial assessment of its criticality. The actual report should be submitted within 72 hours via the FINMA web-based survey and application platform (EHP). The following list contains guidance on the content of such a report to FINMA: a. Name of institution; b. Contact person including contact details	Customers should complete the assessment of the cyberattack and submit a report to the regulatory authorities with the appropriate content and root cause analysis within the specified time frame.	In line with customer compliance requirements, HUAWEI CLOUD has developed a sound incident management process. This process clearly defines the roles and responsibilities for each activity during the incident management process. The priority of events is divided and defined according to the response time and solution time for each priority of event, which is defined according to the degree of impact and scope. After an incident, HUAWEI CLOUD will decide whether to notify customers of the incident based on the extent of the impact it has on or will have on the customer's business. The contents of the notice include, but are not limited to, descriptions of the incident, causes, impacts, actions taken by HUAWEI CLOUD, and

	(telephone and email address); c. Date/time of report to FINMA; d. Date/time when attack was discovered; e. Date/time of attack (if already known); f. Description of cyber attack and current status; g. Initial assessment of severity of the cyber attack (selection: medium, high, severe); h. Severity trend (selection: decreasing, stable, increasing); i. Affected entities (affected organisational unit(s) within the financial institution or service provider); j. Affected protective goals (multiple selection: confidentiality, integrity, availability); k. Affected critical functions, business processes or assets (affected information, technology infrastructure,		measures recommended to customers. HUAWEI CLOUD uses the event platform (CIM) to record and track events, starting from event discovery and ending at event closure. Regular trend analysis of events history and identification of similar events help to find and resolve issues.

	facilities or personnel); l. Affected number of customers (current status); m. Vectors of attack (multiple selection: email, web-based attack, brute force attack, identity theft, removable media, loss/theft of devices, exploitation of software vulnerability, exploitation of hardware vulnerability, etc.); n. Type of attack (description) (e.g. DDoS, unauthorised access, malware, misuse/improper use of technology infrastructure etc.); o. Administrative, operational and/or technical countermeasures with expected time to effectiveness; p. Communication measures (what, to whom, when). 2. If there are new developments or assessments related to the same attack after the reporting obligation has been met in full, a new		

	report must be submitted within the specified deadline of 72 hours. 3. For cyber attacks with the severity levels high and severe, once the financial institution has finished processing the case FINMA expects a conclusive root cause analysis to be submitted including an analysis, reason for the success of the attack, impact of the attack on the observance of regulations, operations and customers as well as mitigating measures to address the consequences of the attack. 4. For cyber attacks with the severity level severe, proof and analyses of the proper functioning of the crisis organisation must also be submitted. 5. For cyber attacks with the severity level medium, a conclusive root cause analysis is sufficient.		

9 Conclusion

This user guide describes how HUAWEI CLOUD provides cloud services that meet the regulatory requirements of the financial industry in Switzerland and shows that HUAWEI CLOUD complies with key regulatory requirements issued by FINMA and SBA. This aims to help customers learn more about HUAWEI CLOUD's compliance with Swiss regulatory requirements of the financial industry to assure customers that they can store and process customer content data safely through HUAWEI CLOUD services. To some extent, this document also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of the Swiss financial industry on HUAWEI CLOUD, and helps customers better shoulder security responsibilities together with HUAWEI CLOUD.

This white paper is for general reference only, and does not have any legal effect or constitute any form of legal advice. Customers should evaluate their own use of cloud services at their discretion, and be responsible for ensuring compliance with relevant financial industry regulatory requirements when using HUAWEI CLOUD.

10 Version History

Date	Version	Description
April 2023	1.0	First release

