HUAWEI CLOUD User Guide to Financial Services Regulations & Guidelines in South Africa

Issue 1.0

Date 2021-06-28

HUAWEI TECHNOLOGIES CO., LTD.

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 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.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Overview

1.1 Background and Purpose of Publication

Following the recent wave of technological development, more and more FIs (Financial Institutions) are planning to transform their business by leveraging high-technology to reduce costs, improve operational efficiency and innovate. To regulate the application of Information Technology (IT) in the financial industry, the Prudential Authority (PA) has issued a series of regulatory directives and guidelines, which put forward relevant regulatory requirements for South African FIs' technology outsourcing management, cloud computing and data offshore management. In addition, the South African Financial Sector Conduct Authority (FSCA) (formerly FSB) issued relevant regulatory directives for insurance outsourcing.

HUAWEI CLOUD, as a cloud service provider, is committed not only to help FIs meeting local regulatory requirements, but also to continuously provide them with cloud services and business operating environments meeting FIs' standards. This whitepaper sets out details regarding how HUAWEI CLOUD assists FIs operating in South Africa in meeting regulatory requirements as to the contracting of cloud services.

1.2 Introduction of Applicable Financial Regulatory Requirements in South Africa

Currently, South Africa adopts the "double-peak regulatory model", and has given two independent regulatory agencies to exercise the regulatory responsibilities of the financial sector:

The Prudential Authority (PA):

The PA is an independent institution established within the management framework of the South African Reserve Bank (SARB). The PA is responsible for the prudential supervision of South African FIs. Its work focuses on maintaining and strengthening the financial security and soundness of FIs and ensuring financial customers are protected from the risks caused by the failure of FIs to fulfill their obligations. The PA has issued relevant directives and guidelines to

regulate the prudential supervision of South African FIs, insurance companies, cooperative FIs.

• **D3/2018: Cloud Computing and the Offshoring of Data (hereinafter referred to as "D3/2018")**:It stipulates the supervision of FIs after they choose cloud computing and/or offshoring of data management. This directive should be considered together with the "G5/2018".

• **G5/2018: Cloud Computing and the Offshoring of Data (hereinafter referred to as "G5/2018")**: It is a guide for the "D3/2018" and should be considered together with the “D3/2018”.

• **G5/2014: Outsourcing of Functions within Banks (hereinafter referred to as “G5/2014”)**: It explains the potential risks arising from the selection of outsourcing service providers by FIs, and provides guidelines for evaluating outsourcing-related risk, and the elements of an appropriate risk management program.

• **G4/2017: Cyber Resilience (hereinafter referred to as “G4/2017”)**: It is a management requirement for the network resilience of FIs, emphasizing the importance of security and effective operations to maintain and promote financial stability and economic growth.

Financial Sector Conduct Authority (FSCA):

Responsible for improving and supporting the efficiency and integrity of the financial market, protecting financial customers, and promoting fair treatment of financial customers. In order to regulate the outsourcing management of FIs, FSCA has issued relevant directives and guidelines:

• **Directive 159.A.i (hereinafter referred to as "Directive 159"):** It is a legislative requirement for outsourcing management of insurance companies (including reinsurance companies). Regardless of whether the insurance company is located in South Africa, or any subsidiary of the insurance company, it shall comply with this directive.

1.3 Definitions

- **HUAWEI CLOUD**

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

- **Customer**

  Registered users having a business relationship with HUAWEI CLOUD.

- **Cloud computing**

  Defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g networks, servers, storage facilities, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- **Offshoring of data**

  Refers to the storage and/or processing of data outside the borders of South Africa.

- **Outsourcing**

Defined as the use of a service provider, whether it is an affiliate within a corporate group or a third party, to perform on a continuing basis a business activity, service, function, or process, which could be undertaken by the FIs, on behalf of the FIs.

- **Insourcing**

  Refers to the outsourcing of functions and activities to a specific institution belonging to a FIs group.

- **Offshoring**

  Refers to the outsourcing by a FIs of a material business activity or function associated with its South African business to a service provider who conducts the outsourced activity outside the borders of South Africa. (That is, regardless of the company's registered place, only the geographic location of the processing activity shall prevail).

- **Material Business Activity or Function**

  Defined as one that has the potential to have a significant impact on the FIs business operations or its ability to manage risks effectively should it be disrupted.

- **Material Incident**

  Refers to a disruption of a business activity, process or function which has, or is likely to have, a severe and widespread impact on the FIs’ operations, services to its customers, or the broader financial system and economy.

- **IT incident**

  Defined as an event, occurrence or circumstance that is not expected or planned as part of the normal operations of FIs and has an effect of disrupting the normal operations of the FIs' IT systems or services.

- **Cyber Incident**

  Any observable occurrence in an information system that (i) jeopardises the cybersecurity of an information system or the information processed, stored or transmitted by the system; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

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 has attained 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.

Certification	Description
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. At present, HUAWEI CLOUD has passed the audit of SOC2 Type 1 Privacy Principle in terms of privacy, which proves that HUAWEI CLOUD has reasonable control measures in terms of cloud management and technology.
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	CSA STAR certification was developed by 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. 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 FusionSphere 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.

Certification	Description
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 specifies 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.
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.
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	Description
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 certificates.
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.
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).
OSPAR certification (Singapore)	OSPAR is an audit report issued by the the Association of Banks in Singapore (ABS) to outsourcing service providers. HUAWEI CLOUD passed the guidelines (ABS Guidelines) of the Association of Banks of Singapore (ABS) on controlling the objectives and processes of outsourcing service providers, proving that HUAWEI CLOUD is an outsourcing service provider that complies with the control measures specified in the ABS Guidelines.

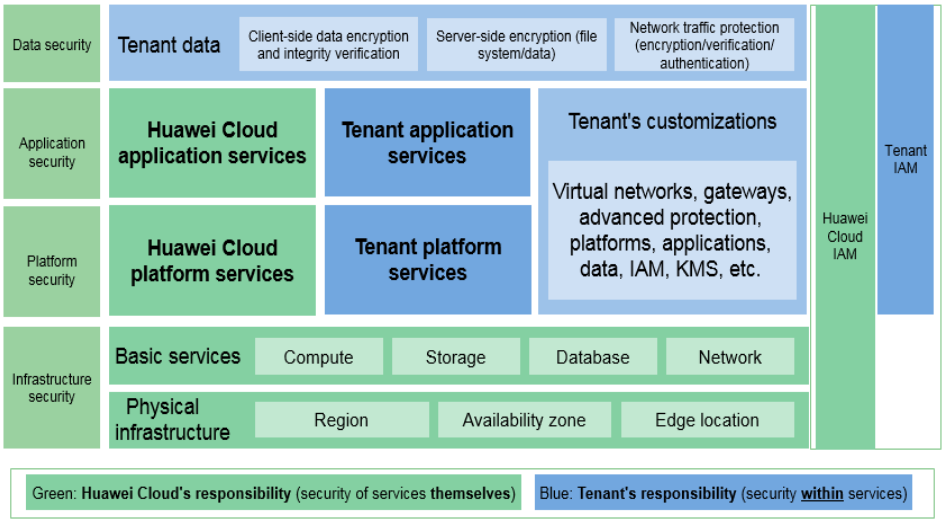
Certification	Description
TISAX (Europe)	TISAX (Trusted Information Security Assessment Exchange) is a security standard for information security assessment and data exchange in the automotive industry launched by the Verband der Automobilindustrie (VDA) and the European Automobile Industry Security Data Exchange Association (ENX). The passing of the TISAX indicates that Huawei Cloud has met the European-recognized information security standards for the automotive industry.

For more information on HUAWEI CLOUD security compliance and downloading relevant compliance certificate, please refer to the official website of HUAWEI CLOUD **"Trust Center - Security 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:

Figure 3-1 Responsibility Sharing Model



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 FIs 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 the requirements of PA " Cloud Computing and the Offshoring of Data "

"D3/2018" and "G5/2018" together elaborated when South African FIs choose to use cloud services or offshoring of data services, the PA supervises related activities and recommendations, and FIs need to deal with matters. "D3/2018" is a directive with legal effect and is a high-level management requirement, "G5/2018" is a guide, which is a landing guide for the "D3/2018" directive.

When FIs are seeking to comply with the requirements provided in the "D3/2018"and "G5/2018", HUAWEI CLOUD, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in the "G5/2018", and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

5.1 The Data Strategy/Framework

Section 4.1 of "G5/2018" requires FIs to develop the data strategy/framework. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response

4.1.1	The Data Strategy/ Framework	The data strategy/ framework should include: 1. how a FIs classifies its data; 2. where (in which jurisdictions) data may be stored (data residency); 3. which service and deployment models of cloud storage are applicable to which classifications of data; 4. which security requirements and restrictions are applicable to the different classifications of data; 5. the process in relation to FIs' data loss and breach requirements.	Customers should formulate and implement data management strategies in accordance with regulatory requirements. HUAWEI CLOUD recommends that FIs first classify data at the data creation stage and conduct risk analysis, and then, based on the results of risk analysis, clarify the storage location, storage services, and security protection measures of the protected data, FIs should distinguish and isolate data at the beginning of the data life cycle. The HUAWEI CLOUD infrastructure is successively built around Regions and Availability Zones (AZ), which can support customers to choose the data storage location according to their needs. In addition to public cloud services, Huawei Cloud also provides customers with private cloud and hybrid cloud solutions. HUAWEI CLOUD provides customers with a range of data storage services, including **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, etc. The services follow advanced industry standards for data security lifecycle management using excellent technologies, practices, and processes in authentication, rights management, access control, data isolation, transmission security, storage security, data deletion, and physical destruction. It also ensures that tenant privacy, ownership and control over their data are not infringed upon, providing users with the most effective data protection. HUAWEI CLOUD has developed a complete emergency contingency plan, which details the organization, procedures

			and operating norms of emergency response, and conducts regular tests to ensure the continuous operation of cloud services and the security of customer business and data.
4.1.2	Asset registration	FIs should maintain a register of all their information assets, including data, IT applications, systems and processes. All such assets should be classified according to the FIs' data classification policy. The location of the data should also be noted and should be in line with data residency requirements as well as information security requirements.	Customers should conduct unified management of their information assets, which should indicate the classification of the corresponding assets and the physical location (country or region) where the data is stored, and identify the requirements for data retention and information security issued by the country or region. HUAWEI CLOUD provides customers with a unified management interface for customers to query and manage their purchased HUAWEI CLOUD resources. Customers can also use the asset management function of Huawei Cloud **Host Security Service (HSS)** for unified management of their assets.

4.1.4	Notification	FIs should have clearly defined data loss and breach processes, including notification and escalation to relevant stakeholders.	Customers should develop a data breach process, which should include requirements and step instructions for notifying and escalation to relevant stakeholders (such as data controllers, data subjects, regulatory agencies, etc.). In order to cooperate with customers to meet the requirements of reporting data loss and breach incidents to relevant stakeholders. HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. According the requirements of laws and regulations, HUAWEI CLOUD timely discloses relevant events, promptly informs customers, and implements emergency plans and recovery procedures to reduce business impact. In addition, HUAWEI CLOUD has established a data breach incident handling mechanism, and the company's legal affairs or local DPO is responsible for identifying data breach-related requirements in applicable laws and regulations. After the incident, the legal affairs or local DPO will approve and report the notification requirements and content.

5.2 Risk Management

Section 4.4 of "G5/2018" requires FIs to develop an effective risk and control frameworks. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response

4.4.1	Risk and control frameworks	1. FIs should ensure that their audit plans and audit work can cover cloud services or offshore data management services provided by service providers 2. Additional assurance work may be triggered by material changes to cloud computing services, data being offshored or compliance requirements, including changes to associated threats and vulnerabilities. 3. When FIs perform audit or assessment, they should include the relevant IT controls of FIs and service providers into the scope of the test to verify the effectiveness of the control.	Customers can adopt methods such as agreement, audit and supervision to ensure that the service provider’s security policies, procedures, and control measures meet the requirements of applicable laws and regulations. If an FI initiates an audit request for HUAWEI CLOUD, HUAWEI CLOUD will arrange responsible personnel to actively cooperate with the audit. Customer audit and supervision interests in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year.

5.3 Prior Risk Assessment

Section 4.5 of "G5/2018" requires FIs to conduct risk assessments before using cloud computing and/or the offshoring of data. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response

4.5.1	Risk Management	1. The risk assessment should identify all risks involved and determine whether adequate controls are in place, or can be implemented, in order for the initiative to be in line with the FIs' risk appetite. 2. FIs should identify, assess, manage, mitigate and report on risks associated with cloud computing and/or the offshoring of data to ensure that they are able to continue to meet their operational and financial obligations to all stakeholders, including customers and regulators. 3. Risks should be adequately understood and managed by FIs prior to entering into a cloud computing or data offshoring arrangement. Factors that should be addressed include continuity, data protection, and prudential and regulatory compliance, and not infringe on the ability of supervisors to execute their prudential duties. 4. The risk assessment should be documented and provide management with sufficient information to be useful for decision making. 5. Responsibility should be assigned for managing the risks identified in the cloud	Customers should conduct risk assessments on the use of Huawei Cloud services in accordance with their risk preferences, the results of the risk assessment should be documented, and the mechanisms (such as evaluation cycles) for monitoring and managing Huawei Cloud services should be determined based on the results of the risk assessment. HUAWEI CLOUD will cooperate with customers in risk assessment work as needed. Technical ability: HUAWEI CLOUD provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. HUAWEI CLOUD has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), HUAWEI CLOUD AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture, HUAWEI CLOUD has created a new multi-computing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the optimal computing power to maximize customer value. Financial strength: HUAWEI CLOUD is Huawei's service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its

		computing and/or the offshoring of data initiative. 6. The risk assessment should be updated as part of monitoring and managing the outsourcing relationship. 7. Part of the risk assessment should entail considering the sustainability of making use of cloud computing and/or the offshoring of data as well as implications for reverting to prior arrangements.	revenue has maintained a strong growth trend. Business reputation: As always, HUAWEI CLOUD adheres to the customer-centric principle, making more and more customers choose HUAWEI CLOUD. HUAWEI CLOUD has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, HUAWEI CLOUD was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. Corporate culture and service policies suitable for FIs: HUAWEI CLOUD defines product safety and functional requirements according to customer business scenarios, laws and regulations, regulatory requirements in product, service planning and design phases. Huawei implements these in R&D, and design phases to meet customer needs. HUAWEI CLOUD has released financial industry solutions to provide end-to-end cloud solutions for banks, insurance companies and other customers, by considering the needs of the industry and Huawei's comprehensive cloud services.

4.5.2	Identification of compliance requirements	FIs should consider where, how and by whom the services are provided. The use of subcontracting and different jurisdictions should not impact on the FIs fulfilling its duties to all its stakeholders, including data residence requirements.	Customers should identify their applicable jurisdictional requirements and make decisions in accordance with jurisdictional requirements (such as identifying data residence requirements in laws and regulations) which service provider should provide services in which country or region, and in what manner. The HUAWEI CLOUD infrastructure is successively built around Regions and Availability Zones (AZ), which can support customers to choose the data storage location configure data residence periods according to their needs.

5.4 Due Diligence

Section 4.6 of "G5/2018" requires FIs to conduct due diligence before using cloud computing and/or the offshoring of data. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.6.1	Due diligence and selection	1. The senior management of the FIs should ensure that the particular service provider is committed to providing, and is able to provide, the required service at agreed levels for the duration of the arrangement. 2. The strength of the service provider's governance, risk and compliance environment should also be assessed before entering into a contract. 3. Factors to consider regarding the due diligence performed include the risks involved, scope, complexity, materiality of the business activity or function, and the reputation and industry standing of the service provider. 4. All investments should adhere to the appropriate governance processes to ensure the strategic fit and business readiness. 5. Where FIs make use of a third-party service provider to provide cloud computing services and/or to offshore	Customers should conduct due diligence before selecting a service provider, especially in terms of governance, risk and compliance management mechanisms. Customers should develop a list of reputable service providers, and be able to identify whether there are any viable alternatives to the preferred service provider. HUAWEI CLOUD provides online version of **HUAWEI CLOUD Service Level Agreement**, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD will assign special personnel to actively cooperate with this due diligence by FIs. Customers' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the situation. HUAWEI CLOUD has obtained ISO27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. Technical ability: HUAWEI CLOUD provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. HUAWEI CLOUD has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. For example, in the field of artificial intelligence (AI), HUAWEI CLOUD AI has landed over 300 projects in 10 major industries, such as city, manufacturing, logistics, internet, medical treatment, and campus. In terms of multi-architecture,

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		data, FIs should have developed a list of reputable service providers which are to be analyzed as part of a due diligence process prior to making the final selection. This should also support the planning of the business continuity processes since the FIs should be able to identify whether there are any viable alternatives to the preferred service provider.	HUAWEI CLOUD has created a new multi- computing cloud service architecture based on "x86 + Kunpeng + Ascend", which enables various applications to run at the optimal computing power to maximize customer value. Financial strength: HUAWEI CLOUD is Huawei's service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue has maintained a strong growth trend. Business reputation: As always, HUAWEI CLOUD adheres to the customer-centric principle, making more and more customers choose HUAWEI CLOUD. HUAWEI CLOUD has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, HUAWEI CLOUD was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. Corporate culture and service policies suitable for FIs: HUAWEI CLOUD defines product safety and functional requirements according to customer business scenarios, laws and regulations, regulatory requirements in product, service planning and design phases. Huawei implements these in R&D, and design phases to meet customer needs. HUAWEI CLOUD has released financial industry solutions to provide end-to-end cloud solutions for banks, insurance companies and other customers, by considering the needs of the industry and Huawei's comprehensive cloud services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.6.2	Business case	1. FIs should have a valid and documented business case for each instance of moving IT services to the cloud computing and/or for the offshoring of data. The business case should clearly identify the link between cloud computing and/or data offshoring and the manner in which it supports the business strategy of the FIs. 2. The business case should clearly define the expected benefits and how these are to be measured. 3. The business case should contain a cost versus benefit analysis. 4. The business case should indicate how the FIs' data strategy is addressed, for instance, in terms of the classification of data as well as data residence.	Customers should formulate business cases for moving IT services to the cloud computing, which should include assessing whether the use of cloud services meets their own business strategy, the expected benefits and cost-benefit analysis process of using cloud services, and data processing strategies. HUAWEI CLOUD provides customers with cloud migration services. Based on the information provided by the customer, HUAWEI CLOUD will negotiate and confirm the specific business goals and scope with the customer, design a migration plan for the customer through demand analysis, and formulate a migration plan and migration exercise.

5.5 Confidentiality, Integrity and Availability

Section 4.7 of "G5/2018" requires FIs to ensure the confidentiality, integrity and availability of their IT assets. The relevant control requirements and HUAWEI CLOUD's responses are as follows.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.7.3	Information security assessment	Regular risk assessments of information security control should be conducted in terms of the importance of the IT system, the nature of the processes or activities involved, the classification of data, the service providers involved, the location of the data, and the cloud deployment model.	Customers should establish a risk assessment framework to regularly assess the risks of outsourcing arrangements. HUAWEI CLOUD can cooperate and actively respond to customer needs. In addition, HUAWEI CLOUD has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve safe and stable operation of the HUAWEI CLOUD environment.
4.7.4	Information security considerations	1. FIs should require service providers contractually agree that third parties will adhere to the information security requirements defined by the FIs. 2. FIs should collect the certifications that service providers have obtained. 3. Contractual agreements defined by FIs should clearly define accountability and penalties in cases where controls are breached, including who would be responsible for losses resulting from a data breach.	Customers should conduct an independent audit or expert assessment of their outsourced service providers on a regular basis, to ensure that service providers provide cloud services under the premise of not less stringent than their own security management requirements. HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. If necessary, FIs can apply to Huawei Cloud for a copy of the audit report through official channels. HUAWEI CLOUD provides online version of **HUAWEI CLOUD Customer Agreement**, which specifies the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.7.5	Assurance and testing	1. The contractual agreement with any third party involved should specify how the FIs will verify adherence to the agreed information security requirements. This may include, but not be limited to, third-party assurance audits as well as any other security testing requirements such as vulnerability scanning and penetration testing. 2. FIs should obtain a copy of the information security policy of any third parties involved in order to determine whether it is in line with the provisions in the FIs' service level agreement (SLA) with the third party.	Customers should ensure that their selected service providers can provide services in accordance with the contract and SLA. HUAWEI CLOUD provides online version of **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. Currently, HUAWEI CLOUD has obtained ISO 27001, ISO 27017, ISO 27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by third parties every year. If necessary, FIs can apply to Huawei Cloud for a copy of the audit report through official channels. To meet customer compliance requirements, HUAWEI CLOUD regularly conducts internal 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. According to ISO 27001, HUAWEI CLOUD has built a perfect information security management system and formulated the overall information security strategy of HUAWEI CLOUD. It clarifies the structure and responsibilities of information security management organization, the management methods of information security system files, and the key directions and objectives of information security, including asset security, access control, cryptography, physical security, operational

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			security, communication security, system development security, supplier management, information security incident management, and business continuity, etc. If a customer applies, HUAWEI CLOUD will provide the customer with a copy of the relevant information security management system as needed.
4.7.6	Security standards	The management requirements for the physical security of the service provider's data center should not be less stringent than the management requirements for the physical security measures that would have been in place had the data been hosted at the FIs' own data centers.	Customers should require the service provider’s physical security management mechanism to be less stringent than that of the FIs. HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures that comply with Class A standard of GB 50174 Code for Design of Electronic Information System Room and T3+ standard of TIA-942 Telecommunications Infrastructure Standard for Data Centers. See Physical and Environmental Security of **HUAWEI CLOUD Security White Paper** for more information.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.7.7	Access control	1. Access rights to information assets in the cloud or offshored data should be restricted in line with the FIs' user access management policies which, for instance, include administrator access to operating systems as well as databases. 2. Third parties involved in either cloud computing and/or data offshoring arrangements should develop and implement adequate user access privilege controls in order to restrict access to the FIs' data, systems and infrastructure. This should be done in a granular fashion and on a least-privilege basis. It remains the responsibility of the FIs to ensure that these controls are in place and are operating efficiently. 3. The FIs remain responsible for ensuring that processes for user provisioning (on-boarding), deprovisioning (termination) and job function changes are	Customers should establish a user access management mechanism to restrict and supervise the access to the system. Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**. Except for support for password authentication, IAM also supports multifactor authentication as an option, and the customer has the option to choose whether to enable it or not. If the customer has a secure and reliable external authentication service provider, the federally authenticated external users of the IAM service can map to the temporary users of HUAWEI CLOUD and access the customer's HUAWEI CLOUD resources. IAM can be authorized by hierarchy and detail as administrators can plan the level of cloud resource access based on the user's responsibilities. They can also restrict malicious access to untrusted networks by setting security policies such as access control lists. In addition, 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. To meet the compliance requirements of customers, HUAWEI CLOUD has established a sound operation and maintenance account management mechanism such that when operational personnel

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		managed in a timely and controlled manner in line with its user access policies.	tries to access Huawei's cloud management network to centralize the management of the system, employee identity account and two- factor authentication are required. All operations accounts are centrally managed, centrally monitored, and automatically audited by LDAP through a unified operational audit platform to ensure that user creation, authorization, and authentication to rights collection processes are fully managed. RBAC permission management is also implemented according to different business dimensions and different responsibilities of the same business to ensure that personnel with different responsibilities in different positions are limited to access the equipment under their role.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.7.8	Encryption	1. FIs should determine the level of encryption required in line with the classification of the data involved in the cloud computing or data offshoring arrangement. With cloud computing, the deployment model followed is also of relevance in determining the appropriate level of encryption. All subsequent encryption considerations should be read in line with the principle that the level of encryption should be commensurate with the materiality of the data and risks involved. 2. FIs would use different classifications, but for any personal, private or confidential data in a multitenant and/or community/ public cloud environment, FIs should consider encrypting data in transit as well as in storage. 3. Where encryption is required, data should be encrypted before it is moved to the cloud and/or	Customers should encrypt and manage personal data, private data or confidential data and other data that needs to be encrypted in accordance with their data classification policies and principles. If customers need move to the cloud, they should consider using industry-approved encryption algorithms and key management mechanisms to encrypt data and properly keep the relevant keys before moving to the cloud. HUAWEI CLOUD services including **Elastic Volume Service (EVS)**, **Object Storage Service (OBS)**, **Image Management Service (IMS)** and Relational Database Service provide data encryption or server-side encryption functions and encrypt data using high-strength algorithms. The server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full-lifecycle key management. Without authorization, others cannot obtain keys to decrypt data, which ensures data security on the cloud. DEW adopts the layered key management mechanism. Hardware security module (HSM) creates and manages keys for customers, which is FIPS 140-2 (Level 2 and Level 3) certified to meet users' data security compliance requirements. Even Huawei O&M personnel cannot obtain the root key. DEW also allows customers to import their own keys as master keys for unified management, facilitating seamless integration with

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		offshored, and the same level of encryption services should be used for data at rest and in motion. 4. Access to encryption keys should be restricted in line with the FIs' key management policies and procedures. Where service providers are involved, key management should be subject to the same level of control as outlined in the FIs' policies and procedures. 5. Policies and procedures should cover public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, recoverability, exchange and storage, where applicable.	customers' services. At the same time, HUAWEI CLOUD adopts a mechanism for online redundant storage of user master keys, multiple physical offline backups of root keys and regular backups to ensure the durability of the keys. See section 6.8.2 Data Encryption Workshop (DEW) of **HUAWEI CLOUD Security White Paper** for more information. For data in transmission, when customers provide Web site services through the Internet, they can use certificate management services provided by the HUAWEI CLOUD United Global Well- known Certificate Service Provider. By applying for and configuring certificates for Web sites, the trusted identity authentication of Web sites and secure transmission based on encryption protocols are realized. In view of the scenario of hybrid cloud deployment and global layout of customer services, we can use the **Virtual private network (VPN)**,**Direct Connect (DC)**, **Cloud Connect (CC)**, and other services provided by HUAWEI CLOUD to realize business interconnection and data transmission security between different regions.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.7.9	Incident management	1. The contractual agreement with any third party involved in cloud computing and data offshoring should refer to the incident management process between the parties, and set out the roles and responsibilities of the respective parties. 2. The incident management process should include incident notifications, responses, remediation, documentation, timelines, addressing the risk of the incident, escalation, and formally closing incidents. 3. The contractual agreement with the service provider should define the types of incidents (for instance data breaches and security violations), events and the actions to be initiated after each incident. 4. FIs should be informed when their data may have been seized or accessed by a foreign country, even if it is through appropriate	HUAWEI CLOUD will not access or use Customer data except as necessary to provide services, or to comply with applicable laws and regulations or a binding order of court or government authority. Customers should establish an information security incident management and specify the roles and responsibilities of both parties in the incident management process in the contract. HUAWEI CLOUD has developed a complete mechanism for internal security incident management and continues to optimize it. The roles and responsibilities are clearly defined for each activity during the incident response process. HUAWEI CLOUD log system based on big data analytics can quickly collect, process, and analyze mass logs in real time and can connect to third- party Security Information and Event Management (SIEM) systems such as SIEM systems provided by ArcSight and Splunk. HUAWEI CLOUD collects management behavior logs of all physical devices, networks, platforms, applications, databases and security systems and threat detection and warning logs of security products and components through a centralized log large data analysis system. In addition, given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 24/7 and a corresponding pool of security expert resources for response. HUAWEI CLOUD also

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		legal processes in that country.	uses a big data security analysis system to communicate alert logs for unified analysis of a variety of security devices. HUAWEI CLOUD formulates the classification and escalation principles of information security incidents, ranking them according to their degree of impact on the customer's business, and initiates a process to notify customers of the incident. When serious events occur on the underlying infrastructure platform and have or may have a serious impact on multiple customers, HUAWEI CLOUD can promptly notify customers of events with an announcement. The contents of the notification include at least but are not limited to a description of the event, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, the incident report will be provided to the customer according to the specific situation. HUAWEI CLOUD annually tests information security incident management procedures. All of information security incident response personnel, including reserve personnel, need to participate. The test scenarios are combined with the current common network security threats, in which high-risk scenarios will be tested during simulations. During the testing process, HUAWEI CLOUD will select test scenarios, develop complete test plans and procedures, and record test results. After their completion, relevant personnel will redact a report and summarize any

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			problems identified during the simulation. If the results are indicating issues with the information security incident management and process, related documentation will be accordingly updated. HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system and information security system. HUAWEI CLOUD maintains a list of contacts that should be contacted in case of an emergency and updates it promptly when notified of personnel changes. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers, such as stipulating the roles and responsibilities of both parties when the incident occurs. HUAWEI CLOUD will promptly notify customers when they may be captured or accessed by institutions outside South Africa in order to comply with laws and regulations or binding orders of government agencies.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.7.10	Multitenancy in the cloud	FIs should consider establishing the security configuration baseline to prevent cross-contamination with other customer environments should be considered.	Customers should develop appropriate security configuration baselines for their cloud environment. In the initial phase, HUAWEI CLOUD will strictly implement the corresponding control measures to ensure HUAWEI CLOUD is secure in its architecture design, equipment selection, host network (for a variety of multi-layer physical and virtual network security isolation methods), access control, border protection technology, configuration, and other aspects for consideration. The **Virtual Private Cloud (VPC)** service provided by HUAWEI CLOUD for customers can create a private network environment for tenants, and realize complete isolation of different tenants in a three-tier network. Tenants have full control over the construction of their own virtual network and configuration, and can configure network ACL and security group rules to strictly control the network traffic coming in and out of subnets and virtual machines, to meet the needs of customers for finer-grained network isolation.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.7.11	Virtualized environments	1. FIs should be aware of the types of virtualization used by service providers and assess whether the level of security within the service provider's environment is adequate or whether it should be augmented by additional security technologies. 2. As part of defining and agreeing on security standards, the security configuration baseline to harden virtualized operating systems should be defined, where applicable. 3. The agreed security standards should further address hypervisor vulnerability management, patch management and release management-specifically when new vulnerabilities are discovered.	Customers need to formulate security configuration baselines for every system and periodically check the baselines. Customers need to assess the risks and develop mitigation measures where the configuration is not compliant with security configuration baselines. HUAWEI CLOUD provides **Host Security Service (HSS)** for customers to identify unsafe items and prevent security risks. HSS can check host baselines, including checking the system password complexity policies, common weak passwords, risky accounts, and common system and middleware configuration. HUAWEI CLOUD has formulated a security configuration baseline for the virtualization operating system to ensure the security when customers using cloud services. The Huawei Product Security Incident Response Team (PSIRT) became an official member of the Forum of Incident Response and Security Teams (FIRST) in 2010, through which Huawei PSIRT and the other 471 members can share incident response best practices and other security information. Huawei PSIRT has a reasonably mature vulnerability response program. The nature of HUAWEI CLOUD's self- service model makes it necessary for PSIRT to continuously optimize the security vulnerability management process and technical means. It will ensure rapid patching of vulnerabilities found on in-house- developed and third party technologies for HUAWEI CLOUD infrastructure, IaaS, PaaS and SaaS services, mitigating risks to tenants'

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			business operations. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD relies on this program and framework to manage vulnerabilities and ensure that vulnerabilities in HUAWEI CLOUD infrastructure and cloud services, and O&M tools, regardless whether they are found in Huawei's or third party technologies, are handled and resolved within SLAs. HUAWEI CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers. Canary deployment or blue-green deployment is used when vulnerabilities are fixed through a patch or version to minimize the impact on tenant services.

5.6 Compliance

Section 4.8 of “G5/2018” requires FIs to ensure that they remain compliant with applicable legislation and regulations when using cloud computing or offshoring of data. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.8.1 4.8.2 4.8.3	Accountability Compliance landscape Compliance in contracts	1) FIs retain accountability for compliance with all legislative requirements and should therefore ensure that a contractual agreement with service providers incorporates the necessary arrangements that will enable them to remain compliant. It further remains the FIs' responsibility to evidence compliance of service process. 2) FIs should identify local laws and regulations applicable to the use of cloud computing or data offshoring arrangements. 3) FIs are responsible for continuously tracking their applicable laws and regulations and updating their own compliance framework regularly when the compliance requirements are updated.	FIs can ensure that the security policies, procedures and control measures of service providers meet the requirements of applicable laws and regulations by means of agreement restriction, examination and supervision, etc. The development of HUAWEI CLOUD business follows Huawei's strategy of "one country, one customer, one policy", and on the basis of compliance with the safety regulations and industry supervision requirements of the country or region where the customer is located. HUAWEI CLOUD not only leverages and adopts best security practices from throughout the industry but also complies with all applicable country-, and region-specific security policies and regulations as well as international cybersecurity and cloud security standards, which forms our security baseline. Moreover, HUAWEI CLOUD continues to build and mature in areas such as our security-related organization, processes, and standards, as well as personnel management, technical capabilities, compliance, and ecosystem construction in order to provide highly trustworthy and sustainable security infrastructure and services to our customers. We will also openly and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			transparently tackle cloud security challenges standing should-to-shoulder with our customers and partners as well as relevant governments in order to meet all the security requirements of our cloud users. HUAWEI CLOUD's services and platforms have been certified by many international and industry security compliance certifications, covering information security, privacy protection, business continuity management, IT service management and other fields. HUAWEI CLOUD is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. In order to meet the compliance requirements of customers, HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system. In addition, HUAWEI CLOUD has a dedicated team to maintain the products descriptions and operating manuals regarding cloud services, and both of them are available in English and accessible on the international website.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			HUAWEI CLOUD receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers.

5.7 Business Continuity

Section 4.10 of “G5/2018” requiring that FIs should have contingency plans for using cloud computing or data offshoring arrangements to ensure business continuity. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.10.1	Capacity	1) Before entering into a contract with a third party, FIs should assess whether the third party has sufficient capacity to effectively manage, on a continuous basis, the services that the FI is planning to move to the cloud and/or offshore. FIs should also consider the potential increased services that the third party may have to provide in the foreseeable future, including the relevant metrics for capacity, such as storage capacity, bandwidth requirements, increased number of users, and transactions per second requirements. 2) Before entering into any third-party contracts, FIs should consider whether the information communications infrastructure between the bank and the third party is sufficient to manage the current and future requirements on a continual basis.	FIs should ensure that their service providers have sufficient capacity to ensure the continuity of their business and possible capacity expansion requirements. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N +1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers. 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

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			prompt measures to ensure the continuous operation of customer cloud services to the greatest extent. In order to meet customer compliance requirements, HUAWEI CLOUD has formulated a standard capacity management and resource forecasting procedure to manage Huawei's cloud capacity as a whole and improve the availability of Huawei's cloud resources. HUAWEI CLOUD resource utilization is monitored daily. Input from all parties provides ongoing predictions for future resource requirements, and resource expansion schemes are formulated to meet these requirements. Business capacity and performance bottlenecks are analyzed and evaluated. When resources reach a preset threshold, a warning is issued, and further solutions are adopted to avoid the impact on the system performance of the tenant cloud service. **Cloud Eye Service (CES)** provides users with a robust monitoring platform for **Elastic Cloud Server (ECS)**, bandwidth, and other resources. CES provides real-time monitoring alarms, notifications, and personalized report views to accurately grasp the status of business resources. Users can set

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			independent alarm rules and notification strategies to quickly see the running status and performance of instance resources of each service.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.10.2	Continuity and recoverability	1. FIs should be able to recover from any failure of a third party within a reasonable time frame, as well as within legal and regulatory imposed timelines. 2. Business continuity requirements, such as recovery time and recovery point objectives (RTOs and RPOs), should be identified through a business impact assessment, documented and, where third parties are involved, agreed with third parties. 3. Disaster recovery and business continuity plans should be developed to maintain continuity of the FIs' operations, including matters related to the recovery from an incident, plans for communicating incidents, and the frequency of testing the adequacy and effectiveness of these plans. 4. Resilience should be designed/built into the FIs' cloud computing and/or data offshoring arrangements. 5. Before contracting with any third party, FIs should consider whether the third party's business continuity measures are commensurate with the FIs' requirements. 6. FIs should have access to the audit or assurance reports of the third party's business continuity plan, including disaster	Customers should establish their own mechanisms for business continuity and develop RTO and RPO metrics to ensure the continuity of their key businesses. If customers need HUAWEI CLOUD's participation in their business continuity plans, HUAWEI CLOUD will actively cooperate. To provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business. In order to meet customer compliance requirements, HUAWEI

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		recovery testing, process audits and control audits at least for activities/ functions managed on their behalf. 7. The third party's business continuity plan should ideally be certified or mapped to internationally recognized standards such as ISO 22301 (business continuity management systems). 8. The roles and responsibilities of the FI and any third party in the event of a disruption should be clearly defined in the contractual arrangements. 9. Contingency plans pertaining to outsourced activities should be reviewed regularly, but not less frequently than once a year.	CLOUD has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N +1 deployment in the data center. Even if one data center fails, it can also balance traffic load to other centers.

5.8 Termination of Services

Section 4.11 of “G5/2018” requires FIs to consider interoperability when services are terminated in their contracts. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.11.1 4.11.2 4.11.4	Planning for termination Contractual agreements Interoperability	1. FIs should avoid being locked into one specific service provider. FIs need to ensure that an exit from a cloud computing and/or offshoring of data arrangement does not affect their compliance with any legislative requirements. 2. The contractual agreement should stipulate the roles and responsibilities for FIs and third parties at the termination of the agreement. 3. The contractual agreement should include a clause to the effect that, upon the termination of the contract, a FIs' data be promptly and completely removed and returned to the FI, transferred to another service provider or destroyed, depending on the nature of the data involved. The contractual arrangements should include sufficient assurance once its data has been removed, transferred or destroyed at the termination of the agreement. 4. FIs should consider interoperability before outsourcing activities to a CSP or data offshoring. 5. FIs should consider in advance and test the option of migrating services to other providers if the selected service provider is no	When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through **Object Storage Migration Service (OMS)** and **Server Migration Service (SMS)** provided by HUAWEI CLOUD, such as migrating to local data center. OMS and SMS support mainstream CSPs at home and abroad, and SMS also supports virtual machine migration and x86 physical server migration (covering about 40 mainstream operating systems). During the destruction of customer data, HUAWEI CLOUD clears the specified data and all the copies. Once customers agree the deletion, HUAWEI CLOUD deletes the index relationship between customers and data, and clears the storage space, such as memory and block storage before reallocation, to ensure that related data and information cannot be restored. If a physical storage medium is to be disposed, HUAWEI CLOUD clears the data by degaussing, bending, or breaking the storage medium to ensure that data on the storage medium cannot be restored.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		longer able to meet its contractual obligations. 6. FIs should have contingency plans for the outsourcing service environment in place to continue with its operations in case of an unforeseen event.	

5.9 Forensic Investigation

Section 4.12 requires FIs to specify forensic investigation requirements when using cloud computing or data offshore arrangements. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.12.1	Applicability	Any cloud computing and/or offshoring of data arrangements must not impact on a FIs' ability to conduct forensic audits or investigations: 1. FIs should identify the risks to cloud /offshore data that may arise due to forensics and develop appropriate control measures to ensure that is not lower than the risk appetite of FIs. 2. Ensure the integrity of data in cloud or offshore management during forensics.	Customers should formulate the cloud forensics process and control measures according to their risk preferences to ensure the confidentiality, integrity and availability of data during cloud forensics. HUAWEI CLOUD strictly adheres to "not accessing customer data without permission" and 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. In addition, the server-side encryption function integrates Key Management Service (KMS) of HUAWEI CLOUD **Data Encryption Workshop (DEW)**, which provides full-lifecycle key management. Without authorization, no one except the customer can obtain keys to decrypt data, which ensures the confidentiality, integrity and availability of the data in the process of cloud forensics.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.12.2	Contractual agreements	The contractual agreement with the third parties must clearly prescribe: 1. The access that the FIs, regulatory authorities and law enforcement agencies would have in order to conduct forensic audits and investigations; 2. Controls should be deployed to prove that evidence has not been tampered with; 3. Define the roles and responsibilities for both parties in terms of forensic data; 4. Determine which forensic tools are available to directly or via the third party; 5. Stipulate both parties' responsibilities related to discovery searches, litigation holds, preservation of evidence and expert testimony; 6. Stipulate the duration during which forensic data would be available; 7. Stipulate the ways in which service providers preserve FIs' data.	Customers should formulate contracts with CSPs according to relevant requirements. HUAWEI CLOUD provides online **HUAWEI CLOUD Customer Agreement**, which specifies the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. Customer's audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the HUAWEI CLOUD according to the situation.

5.10 Contractual Agreements

Section 4.13 of "G5/2018" requires FIs to consider the contents of contract agreements when using cloud computing or data offshore arrangements. The relevant control requirements and HUAWEI CLOUD's responses are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.13	Contractual agreements	The contractual agreement with the third parties must clearly prescribe: 1. The ownership rights of FIs' data and how the ownership rights are affected by the different laws of the countries which will host the data; 2. The data can only be stored in the geographical location specified in the contract that meets the requirements of applicable laws and regulations; 3. Which activity can be subcontracted by service providers, and subcontracting should also be carried out in accordance with the main contract; 4. The service provider shall provide an undertaking to treat the FIs' data with the utmost confidentiality at all times and to ensure that its employees and service providers adhere to the same standard of confidentiality. Access should be restricted on a least-privilege basis. 5. Define roles and responsibilities in case of a data breach, including cooperative processes to be implemented during the investigation, and the disclosure notice or other legal compliance obligations; 6. Service providers should not inhibit the FIs' ability to meet its data retention legal requirement.	Customers should formulate contracts with CSPs according to relevant requirements. HUAWEI CLOUD provides online **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. For example, the operation of cloud service providers is audited by independent auditors, the conditions and responsibilities for HUAWEI CLOUD to subcontract services to other suppliers.

6 How HUAWEI CLOUD Meets the Requirements in PA “Outsourcing of functions within banks”

Prudential Authority (PA) released “G5/2014” in July 2014, it is mainly used to help FIs judge whether it is a “material business activity or function” and the risks that may arise after the activity or function is outsourced.

When FIs are seeking to comply with the requirements of “G5/2014”, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following materials summarize the compliance requirements related to cloud service providers in “G5/2014”, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
4.5	Notify the Office	This Office (The Office of the Registrar of Banks) would like to emphasize that FIs should realize the significance of cloud computing initiatives and offshoring of material IT business activities and functions. FIs should notify this Office prior to offshoring material business activities.	Customers should identify the use of CSP or offshore outsourcing services as outsourcing of "material business activities or functions" and inform The Office of the Registrar of Banks in South Africa of the outsourcing activities before outsourcing. HUAWEI CLOUD will cooperate with customers to provide relevant reporting materials and cooperate with customers to meet the regulatory notice. In addition, HUAWEI CLOUD provides an after-sales service guarantee for customers, the HUAWEI CLOUD professional service engineer team provides 24/7 service support. Customers can seek help through work orders, intelligent customer service, self-service, and telephone. In addition to basic support, customers with complex systems can choose from the tiered support plans to obtain exclusive support from personnel such as the IM enterprise group, Technical Service Manager (TAM), and service manager.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
6.4	Due diligence and selection	FIs should conduct an evaluation of and perform the necessary due diligence on a prospective service provider prior to entering into an outsourcing agreement. Service provider factors to be considered during a due diligence exercise include business background and reputation, conflicting contractual arrangements with other persons, strategy and goals, fee structure and incentives, financial performance and condition, human resource management, incident reporting and management programmes, information security, insurance coverage, jurisdictional issues and sovereign risks (cross border activities), legal and regulatory compliance, management of information systems, operations and internal controls, physical security, qualifications/ backgrounds/reputations of company principals, reliance on subcontractors, resilience and risk management.	Customers should conduct an evaluation of and perform the necessary due diligence on a prospective service provider prior to entering into an outsourcing agreement. If an FI initiates an audit or due diligence request for HUAWEI CLOUD, HUAWEI CLOUD will arrange a responsible person to actively cooperate regarding the audit or due diligence. Technical capabilities: HUAWEI CLOUD provides cloud services online, opening Huawei's technology accumulation and product solutions in ICT infrastructure for more than 30 years to customers. HUAWEI CLOUD has five core technological advantages: full stack scenario AI, multidimensional framework, extreme performance, security and reliability, and open innovation. Financial soundness: HUAWEI CLOUD is Huawei's service brand. Since its launch in 2017, HUAWEI CLOUD has been developing rapidly and its revenue has maintained a strong growth trend. Business reputation: As always, HUAWEI CLOUD adheres to the

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			customer-centric principle, making more and more customers choose HUAWEI CLOUD. HUAWEI CLOUD has made breakthroughs in different Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. Apart from Chinese mainland, HUAWEI CLOUD was launched in Hong Kong (China), Russia, Thailand, South Africa and Singapore in succession. Compatibility with FIs' corporate culture and service policies: HUAWEI CLOUD defines product safety and functional requirements according to customer business scenarios, laws and regulations, regulatory requirements in product and service planning, and design phases. Huawei implements these in R&D, and design phases to meet customer needs. HUAWEI CLOUD has released financial industry solutions to provide end-to-end cloud solutions for banks, insurance companies and other customers, by considering the needs of the industry and

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			Huawei's comprehensive cloud services.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
6.5	Outsourcing contract	1. The contract and SLAs should be reviewed by the FI's legal counsel before being signed and the contract and SLAs should include the following aspects: Access to assets, audit (including right to audit) and monitoring procedures, business disruption and contingency plans, commencement and end dates, confidentiality/integrity/privacy and security of information, customer complaints, default arrangements and termination provisions, dispute resolution arrangements, establishment and monitoring of performance standards, foreign based services, incentive compensation review, indemnification, insurance, limits and liability, notification of financial difficulty/ catastrophic events, and significant incidents, offshoring arrangements, ownership and license issues, pricing and fee structure, provisions for amendment, provisions for periodic reviews, remedies (including early-exit options) for non-performance, reporting requirements, responsibilities for providing/ receiving and retaining information, responsibility for compliance with applicable laws and regulations, review provisions, rights of regulatory and supervisory authorities(including unrestricted access to information), roles, rights and responsibilities, scope and nature of the arrangement and services to be supplied, service levels and performance requirements, subcontracting.	Customers should formulate contracts with CSPs according to relevant requirements. HUAWEI CLOUD provides online **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement,** which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. For example, the operation of cloud service providers is audited by independent auditors, the conditions and responsibilities for HUAWEI CLOUD to subcontract services to other suppliers.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		2. FIs that outsource a material business activity or function must ensure that their outsourcing agreement includes an indemnity to the effect that any subcontracting by a third-party service provider of the outsourced function will be the responsibility of the third-party service provider, including liability for any failure on the part of the sub-contractor. FIs are expected to address all issues relevant to managing the risks associated with each outsourcing arrangement to a feasible and reasonable extent. All legal documents should be stored in accordance with the FIs' legal document management procedures.	

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
6.6	Managing and monitoring the relationship	FIs should ensure they have sufficient and appropriate resources to manage and monitor the outsourcing relationship at all times. Personnel with oversight and management responsibilities for service providers should have the appropriate level of expertise. Monitoring activities should include the following: 1. Verifying that the integrity of the systems and controls of the service provider are maintained. 2. Remaining aware of any problems, including financial concerns, encountered with a service provider. 3. Maintaining appropriate levels of regular contact with the service provider, ranging from daily operational contact to senior management involvement. 4. Regular monitoring of performance under the agreement. 5. Escalation of issues identified.	Customers should manage and monitor the cloud services they use to ensure that suppliers can provide sufficient resources and services according to relevant requirements. HUAWEI CLOUD's services and platforms have been certified by many international and industry security compliance certifications, covering information security, privacy protection, business continuity management, IT service management and other fields. HUAWEI CLOUD is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. HUAWEI CLOUD receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. In addition, HUAWEI CLOUD provides an after-sales service guarantee for customers, the HUAWEI CLOUD professional service engineer team provides 24/7 service support. Customers can

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			seek help through work orders, intelligent customer service, self-service, and telephone. In addition to basic support, customers with complex systems can choose from the tiered support plans to obtain exclusive support from personnel such as the IM enterprise group, Technical Service Manager (TAM), and service manager.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
6.7	Contingency planning and business continuity	FIs should formulate contingency plans and preplans for outsourcing any functions and review them not less frequently than once a year. The contingency plan shall at least include the following contents: 1. Consider the availability of alternative service providers and hand-over procedures to new service providers. 2. Determine the procedures that need to be in place to ensure minimum disruption to business when an alternative service provider is sought. 3. Ensure that the bank has in its possession, or can readily obtain, all records necessary to allow it to sustain business operations, meet its statutory obligations, and provide all information necessary for the bank to meet its mandate. 4. Ensure that a disaster recovery and business continuity plan is in place for the contracted services and products. 5. Assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to their own plan. 6. Document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans. 7. Periodically obtain evidence of testing that the service provider's business continuity and contingency plans are adequate and effective. 8. Maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform.	Customers should establish their own mechanisms for business continuity and develop RTO and RPO metrics to ensure the continuity of their key businesses. If customers need HUAWEI CLOUD's participation in their business continuity plans, HUAWEI CLOUD will actively cooperate. To provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills and tests regularly to continuously optimize emergency response. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
		9. Consider requirements should the bank wish to or need to reinstate an outsourced function or activity in-house.	regarded as an important criterion to judge key business. In order to meet customer compliance requirements, HUAWEI CLOUD has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity management system. Customers can rely on the Region and Availability Zone (AZ) architecture of HUAWEI CLOUD Data Center cluster for disaster recovery and backup of their business systems. Data centers are deployed around the world according to rules. Customers have disaster data backup centers through two places. If a failure occurs, the system automatically transfers customer applications and data from the affected areas to ensure business continuity on the premise of meeting compliance policies. HUAWEI CLOUD has also deployed a Global Server Load Balance Center. Customer applications can achieve N+1 deployment in the data center. Even if one data center fails, it can

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			also balance traffic load to other centers. When the service agreement terminates, customers can migrate content data from HUAWEI CLOUD through **Object Storage Migration Service (OMS)** and **Server Migration Service (SMS)** provided by HUAWEI CLOUD, such as migrating to local data center.
6.9	Supervisory access to information	The outsourcing agreement signed between the FIs and the service provider should include the right for The Office of the Registrar of Banks to access information, which includes conducting on-site visits at the service provider should this Office consider it necessary in its role as prudential supervisor. Should management become aware of any possible restriction on the provision of information relating to the outsourced function, this Office has to be informed thereof.	Customers should formulate contracts with CSPs according to relevant requirements. HUAWEI CLOUD provides online **HUAWEI CLOUD Customer Agreement** and **HUAWEI CLOUD Service Level Agreement**, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD has also developed an offline contract template, which can be customized according to the needs of different customers. For example, the right of the Office to conduct on-site visits of HUAWEI CLOUD.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
6.10	Assessments of outsourcing	1. The management of a FI should ensure that the FI has processes in place to identify and deal with any weakness in a service provider's performance that may have an adverse impact on the service provided to the FI. This may include access to the service provider by the FI’s internal and external auditors, as well as access by external persons conducting independent reviews for assessment by management. 2. The FI’s management should ensure that there is capacity to address problems that arise from investigations conducted at the service provider and that appropriate actions are taken when required. 3. A FI’s internal audit function should review the FI’s material outsourcing business activities to verify that it is in line with its outsourcing policy and should report these results to the board or board audit committee. This Office may request a FI’s external auditor, or an appropriate external expert, to provide an assessment of the risk management processes in place with respect to an arrangement to outsource a material business activity or function. Such an assessment could cover areas such as IT systems, data security, internal control frameworks and business continuity plans. Such reports will be paid for by the FI and are to be made available to this Office if and when required.	Customers should establish processes and mechanisms for outsourcing management to ensure that risks related to outsourcing are properly identified and controlled. This Office may request a customer’s external auditor, or an appropriate external expert, to provide an assessment of the risk management processes in place with respect to an arrangement to outsource a material business activity or function. Such reports will be paid for by the customer and are to be made available to this Office if and when required. HUAWEI CLOUD's services and platforms have been certified by many international and industry security compliance certifications, covering information security, privacy protection, business continuity management, IT service management and other fields. HUAWEI CLOUD is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. HUAWEI CLOUD receives regular

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. If the customer needs to conduct supervision and reporting, HUAWEI CLOUD will cooperate with the customer to provide relevant materials.

7 How HUAWEI CLOUD Meets the Requirements of PA “Reporting of material information technology and/or cyber incidents”

Prudential Authority (PA) released “D2/2019” in September 2019, this Directive sets out the Prudential Authority's reporting requirements in relation to material information technology and/or cyber incidents.

When FIs are seeking to comply with the requirements of “D2/2019”, HUAWEI CLOUD, as a cloud service provider, may participate in some activities involved in the requirements. The following materials summarize the compliance requirements related to cloud service providers in “D2/2019”, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
2.1	Directive	1. FIs should establish and maintain robust governance structures to ensure adequate management and operational oversight over critical business functions, resources and infrastructures; 2. FIs should establish a sound event management process to manage and report IT and cyber incidents; 3. After a material IT or cyber incidents occurs, the FIs shall notify PA within one day (the "Material IT and cyber incident report" form shall be filled out and submitted to **SARB-PA-ITIncidentReporting@resbank.co.za**); 4. The FIs shall submit the root cause analysis and impact analysis report to PA within 14 calendar days from the date of notification to PA.	Customers should establish an event management process for managing and reporting IT and cyber incidents. Customers should clearly report to PA within one day of material IT events or cyber incidents and submit the root cause analysis and impact analysis report to PA within 14 calendar days after reporting. To cooperate with customers to meet the requirements of reporting material IT events and cyber incidents to PA, HUAWEI CLOUD has set up a 24/7 professional safety incident response team and expert resource pool. According to the requirements of laws and regulations, relevant events are disclosed promptly, customers are informed promptly, and emergency plans and recovery processes are implemented to reduce business impact.

8 How HUAWEI CLOUD Meets the Requirements of Cyber Resilience of PA

SARB-PA issued G4/2017 Cyber Resilience Rules (G4/2017 for short) in May 2017. This guidance is based on the internationally accepted GUIDANCE ON CYBER RESILIENCE FOR FINANCIAL MARKET INFRASTRUCTURES (FMIs) to the South African FIs regarding cyber resilience requirements.

When FIs are seeking to comply with the requirements provided in the G4/2017, HUAWEI CLOUD, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in G4/2017 and corresponding in the GUIDANCE ON CYBER RESILIENCE FOR FINANCIAL MARKET INFRASTRUCTURES, and explains how HUAWEI CLOUD, as a cloud service provider, can help FIs to meet these requirements.

No.	Control Domain	Specific Control Requirements in G4/2017	Specific Indicators in GUIDANCE ON CYBER RESILIENCE FOR FMIs	HUAWEI CLOUD Response
2.3.3	Recovery Time	The recovery time objectives for FIs should be based on a thorough business impact assessment and take all other relevant legislative and regulatory requirements into consideration. In addition, high availability and failover should be taken into account when designing resilience principles to minimize the impact on customers.	6.2.2 Resumption within two hours (i.e. two-hour RTO). Objectives for resuming operations set goals for, ultimately, the sound functioning of the financial system, which should be planned for and tested against. FMIs should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios.	Customers should establish their own business continuity mechanisms and formulate RTO and RPO indicators to ensure their key businesses, and the RTO of the financial system should be no less than 2 hours. If customers need HUAWEI CLOUD's participation in the process of running their internal business continuity plans, HUAWEI CLOUD will actively cooperate. To provide continuous and stable cloud services to customers, HUAWEI CLOUD has obtained ISO 22301 certification and formulates business continuity management systems for the cloud to suit the customer's business needs. HUAWEI CLOUD carries out business continuity promotion and training within the organization every year, and conducts emergency drills

No.	Control Domain	Specific Control Requirements in G4/2017	Specific Indicators in GUIDANCE ON CYBER RESILIENCE FOR FMIs	HUAWEI CLOUD Response
				and tests regularly to continuously optimize emergency response. Under the requirements of this framework, HUAWEI CLOUD carries out regular business impact analysis, identifies key business, and determines the recovery target and minimum recovery level of key business. In the process of identifying key business, the impact of business interruption on cloud service customers is regarded as an important criterion to judge key business. In order to meet customer compliance requirements, HUAWEI CLOUD has formulated a sound recovery strategy for key businesses supporting the continuous operation of cloud services according to the requirements of its internal business continuity

No.	Control Domain	Specific Control Requirements in G4/2017	Specific Indicators in GUIDANCE ON CYBER RESILIENCE FOR FMIs	HUAWEI CLOUD Response
				management system. Customers rely on the multi-region and multi-available area (AZ) architecture of HUAWEI CLOUD data center cluster to achieve the flexibility and availability of their business systems. Data centers are deployed around the world, so customers will have mutual disaster data backup centers in case of disasters. In the event of one failure in an area, the system automatically transfers customers applications and data away from the affected area to a data backup center, while meeting compliance policies, to ensure business continuity for affected customers. HUAWEI CLOUD also deploys a global load-balanced management center, where the

No.	Control Domain	Specific Control Requirements in G4/2017	Specific Indicators in GUIDANCE ON CYBER RESILIENCE FOR FMIs	HUAWEI CLOUD Response
				customers' applications enable N1 deployment sizing in the data center while balancing traffic load to other centers, even in the event of a data center failure.

No.	Control Domain	Specific Control Requirements in G4/2017	Specific Indicators in GUIDANCE ON CYBER RESILIENCE FOR FMIs	HUAWEI CLOUD Response
2.3.4	Security Testing	With regards to security testing, specifically also referring to penetration testing, when using third parties, FIs are required to make use of reputable external service providers for such testing which may, for instance, be evidenced through certification or accreditation.	7.2.2 FMIs should carry out penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes. To provide an in-depth evaluation of the security of FMIs' systems, those tests should simulate actual attacks on the systems. Penetration tests on internet-facing systems should be conducted regularly and whenever systems are updated or deployed. Where applicable, the tests could include other internal and external stakeholders, such as those involved in business continuity, incident and crisis response teams, as well as third parties, such as service providers and participants.	Customers should establish an effective security testing system and regularly conduct security testing on key information systems. To meet customer compliance requirements, HUAWEI CLOUD regularly conducts internal 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.

No.	Control Domain	Specific Control Requirements in G4/2017	Specific Indicators in GUIDANCE ON CYBER RESILIENCE FOR FMIs	HUAWEI CLOUD Response
2.3.5	Situational Awareness	The FIs' situational awareness must include cyber threat intelligence which is applicable to the local market and its operations in South Africa.	8.2.1 Identification of potential cyber threats. An FMI should identify cyber threats that could materially affect its ability to perform or to provide services as expected, or that could have a significant impact on its ability to meet its own obligations or have knock-on effects within its ecosystem, and should regularly review and update this analysis. 8.2.2 Threat intelligence process. An FMI should establish a process to gather and analyze relevant cyber threat information. 8.2.4 Effective use of information. FMIs should use cyber threat intelligence to implement resilience measures and inform the prioritization of resources, risk mitigation	Customers should establish a situational awareness management mechanism to ensure that the information and information processing facilities in the network are protected. The Huawei Product Security Incident Response Team (PSIRT) became an official member of the Forum of Incident Response and Security Teams (FIRST) in 2010, through which Huawei PSIRT and the other 471 members can share incident response best practices and other security information. Huawei PSIRT has a reasonably mature vulnerability response program. The nature of HUAWEI CLOUD's self-service model makes it necessary for PSIRT to continuously optimize the security

No.	Control Domain	Specific Control Requirements in G4/2017	Specific Indicators in GUIDANCE ON CYBER RESILIENCE FOR FMIs	HUAWEI CLOUD Response
			strategies and training program.	vulnerability management process and technical means. It will ensure rapid patching of vulnerabilities found on in-house-developed and third party technologies for HUAWEI CLOUD infrastructure, IaaS, PaaS and SaaS services, mitigating risks to tenants' business operations. In addition, Huawei PSIRT and HUAWEI CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, identification, response, and disclosure. HUAWEI CLOUD manages vulnerabilities based on its vulnerability management system to ensure that vulnerabilities on self-developed and third-party infrastructure, platforms,

No.	Control Domain	Specific Control Requirements in G4/2017	Specific Indicators in GUIDANCE ON CYBER RESILIENCE FOR FMIs	HUAWEI CLOUD Response
				application layers, cloud services, and O&M tools are detected and fixed within the time specified in SLA. This reduces risks caused by malicious exploitation of vulnerabilities and adverse impacts on customers businesses. See section 8.2 Vulnerability Management of **HUAWEI CLOUD Security White Paper** for more information.

9 How HUAWEI CLOUD Meets the Requirements of “159.A.i” of FSCA

FSCA issued “159.A.i” in April 2012.This directive is a legislative requirement for the outsourcing management of all insurers (including reinsurers) in South Africa.

When South Africa insurers are seeking to comply with the requirements provided in the “159.A.i”, HUAWEI CLOUD, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following content summarizes the compliance requirements related to cloud service providers in “159.A.i”, and explains how HUAWEI CLOUD, as a cloud service provider, can help insurers to meet these requirements.

9.1 Internal Review and Approvals

Section 7.5 of the “159.A.i” requires insurers to consider related outsourcing risks when planning outsourcing. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.5	Internal Review and Approvals	An insurer must prior to outsourcing any aspect of its insurance business - 1. assess the costs and benefits and potential risk inherent in the proposed outsourcing; 2. assess how the insurer's risk profile will be affected by the outsourcing; 3. identify potential third parties to undertake the outsourcing through objective procurement and selection procedures; 4. consider the potential impact of multiple outsourcing arrangements provided by the preferred third party to a number of insurers; 5. assess whether the third party is fit and proper; 6. assess the preferred third party's governance, risk management, and internal controls and its ability to comply with applicable laws; 7. assess the preferred third party' service capability and financial viability; 8. develop appropriate management and monitoring procedures for the proposed outsourcing; 9. develop appropriate contingency plans to ensure the continuous functioning of the insurance business of the insurer in the event that the outsourcing arrangement is terminated or ineffective.	Customers should conduct risk assessments on their outsourced businesses and preferred service providers to identify potential risks. HUAWEI CLOUD can cooperate and actively respond to customer needs. In addition, HUAWEI CLOUD has developed a complete information security risk management mechanism, regular risk assessment and compliance review to achieve safe and stable operation of the HUAWEI CLOUD environment.

9.2 Written Contracts

Section 7.6-7.7 of the "159.A.i" requires insurers to consider the content of the contract when planning outsourcing. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.6 7.7	Written Contracts	All outsourcing must be governed by written contracts that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities, and expectations of all parties. A written contract must - 1. specify the level and standard of service that must be rendered to a policyholder, where relevant, and to the insurer; 2. require that the third party have appropriate governance, risk management, and internal controls in place to perform the outsourced process, service or activity; 3. provide for the type and frequency of reporting by the third party on the process, service or activity performed under the contract; 4. specify that the insurer has continued access to information relating to the outsourced process, service or activity; 5. require that the third party comply with applicable laws, including POPIA; 6. address confidentiality, privacy and the security of information of the insurer and policyholders; 7. provide for business contingency processes.	Customers should formulate a contract with the cloud service provider in accordance with relevant requirements and sign a written contract. HUAWEI CLOUD has developed an offline contract template, which can be customized according to the needs of different customers. HUAWEI CLOUD has identified and analyzed the requirements of the POPIA. For more information, please see **HUAWEI CLOUD Compliance with South Africa POPIA**.

9.3 Management and Regular Review

Section 7.9-7.11 of the "159.A.i" requires insurers to regularly review the risks associated with any outsourcing. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
7.9 7.10 7.11	Management and regular review	1. An insurer must ensure that the level and standard of service of any outsourcing are appropriately monitored, managed, and regularly reviewed. 2. An insurer must regularly assess the third party's governance, risk management, and internal controls (including fit and properness); ability to comply with applicable laws; and service capability and financial viability.	Customers should ensure that service providers can provide cloud services in accordance with the agreements and standards in contracts and SLAs, and regularly evaluate the management, compliance, and operation status of service providers. HUAWEI CLOUD's services and platforms have been certified by many international and industry security compliance certifications, covering information security, privacy protection, business continuity management, IT service management and other fields. HUAWEI CLOUD is committed to creating security and credible cloud services for customers in all walks of life and providing empowerment and escorting services for customers. In order to meet the compliance requirements of customers, HUAWEI CLOUD regularly audits and updates all system documents every year according to the requirements of the internal business continuity management system. In addition, HUAWEI CLOUD has a dedicated team to maintain the products descriptions and operating manuals regarding cloud services, and both of them are available in English and accessible on the international website. HUAWEI CLOUD receives regular audits from

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
			professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit activities initiated by customers. In addition, HUAWEI CLOUD provides an after-sales service guarantee for customers. HUAWEI CLOUD professional service engineer team provides 24/7 service support so customers can seek help with methods such as work orders, intelligent customer service, self-service, and telephone. In addition to basic support, customers with complex systems can choose from the tiered support plans to obtain exclusive support from personnel such as the IM enterprise group, Technical Service Manager (TAM), and service manager.

9.4 Notification of Outsourcing of Material and Management Functions

Section 8.1-8.2 of the "159.A.i" requires insurers to notify supervision when important functions are outsourced. The relevant control requirements and HUAWEI CLOUD's response are as follows:

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
8.1 8.2	Notification of outsourcing of material and management functions	1. An insurer must timeously, prior to entering into an outsourcing contract, notify the Registrar of – the proposed outsourcing of a management, control or material function (subject to any requirements under the Acts); the details of the third party to whom the insurer will outsource that function; and the key risks associated with the outsourcing and the risk mitigation strategies that will be put in place to address these risks. 2. An insurer must immediately notify the Registrar of any material developments (such as termination, material non-performance and the like) with respect to the outsourcing during the duration of the outsourcing contract.	If customers are involved in migrating important systems to the cloud, they are within the scope of this requirement (for example, the interruption of public cloud services will have an impact on the operations of insurance customers). Before such outsourcing, the customer should notify the Registrar. HUAWEI CLOUD will cooperate with customers to provide relevant reporting materials, and cooperate with customers to notify the Registrar.

10 Conclusion

This whitepaper describes how HUAWEI CLOUD provides cloud services that meet regulatory requirements of the financial industry in South Africa and shows that HUAWEI CLOUD complies with key regulatory requirements issued by the PA and FSCA. This aims to help customers learn more about HUAWEI CLOUD's compliance status with South Africa's regulatory requirements related to the financial industry and to assure customers that they can store and process customers' content data securely. To some extent, this whitepaper also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of the South Africa's financial industry on HUAWEI CLOUD, and assists customer to better identify security responsibilities together with HUAWEI CLOUD.

This whitepaper is for reference only and does not have legal effect or constitute any legal advice. Customers should assess their own use of cloud services as appropriate and ensure compliance with relevant regulatory requirements from the South Africa's financial industry when using HUAWEI CLOUD.

11 Version History

Date	Version	Description
May 2021	1.0	First release

