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

Issue 1.0

Date 2022-08-09

HUAWEI

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

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

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Overview

1.1 Background and Purpose of Publication

With the development of technology, the use of cloud computing has become the normal condition of Financial Institutions (FIs) in Nigeria. Cloud computing brings great benefits to the development of FIs, but it also creates a complex environment for FIs. To regulate the application of Information Technology (IT) in the financial industry, the Central Bank of Nigeria（CBN） published a series of regulatory requirements and guidelines, covering cyber security and IT risk management for FIs operating in Nigeria.

HUAWEI CLOUD, as a cloud service provider, is committed not only to helping FIs meet local regulatory requirements, but also to continuously providing them with cloud services and business operating environments meeting FIs' standards. This white paper sets out details regarding how HUAWEI CLOUD assists FIs operating in Nigeria to meet regulatory requirements when providing cloud services.

1.2 Introduction of Applicable Financial Regulatory Requirements in Nigeria

CBN, the Nigerian financial services regulator that oversees and regulates cybersecurity defense for banks and non-financial institutions, has issued relevant guidelines to regulate this area.

- **Nigeria Financial Services Industry IT Standards Blueprint（Blueprint）:** CBN released the Nigeria Financial Services Industry IT Standards Blueprint in July 2019. This document encourages FIs in Nigeria to develop, grow and sustain competency in Information Technology. It hopes to achieve this by serving as a framework and guide for the use of and implementation of Information Technology and Information Technology (IT) Standards. The overall objective is to bring Nigerian Financial Institutions to an acceptable minimum level of process maturity, which will help drive sustainable growth, build resilience and improve customer experience.
- **Risk-based Cybersecurity Framework and Guidelines For Deposit Money Banks and Payment Service Providers（DBM and PSP Guidelines）:** An increase in the number and sophistication of threats targeting DMB and PSP in general led to the promulgation of the CBN's DBM and PSP Guidelines. The

guidelines, which came into effect on January 1, 2019 and was designed to provide guidance for DMB and PSP to implement network security programs, outline minimum requirements for enhancing the cybersecurity of banks and payment service providers so that they remain resilient and proactively seek to secure their critical information assets.

- **Draft Risk-based Cybersecurity Framework and Guidelines For Other Financial Institutions (Draft OFI Guidelines):** CBN released the Draft Risk-based Cybersecurity Framework and Guidelines For Other Financial Institutions (OFIs) in Nigeria on August 13, 2021. The guidance outlines the minimum requirements that OFIs must adhere to when developing and implementing strategies, policies, procedures and related activities aimed at mitigating cyber risks.

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.

- Service provider

An entity, including its branches providing services to a FI under an

outsourcing arrangement.

- Cloud computing

Cloud computing refers to a type of internet-based computing that provides

shared computer processing resources and data on demand according to the National Institute of Standards and Technology (NIST).

- critical system

“critical system” shall mean any IT infrastructure (servers, applications, databases, network, ATM, POS, etc.) whose unavailability (such as failure, unplanned downtime, etc.), corruption, unauthorized access and/or interception of the information it stores, processes or transmit will results in a significant financial loss and negatively impact business operation and service to customers.

- Cyber-Incident

A Cyber-Incident is referred to as any incident which may result in a significant financial loss as a result of:

1. Unplanned outage of IT system(s) such as Core Banking Application, Treasury Systems, Trade finance systems, core network devices, Internet banking systems, electronic channels (e.g. ATMs, POS, USSD, Mobile banking, etc.) and connected payment systems e.g. SWIFT, RTGS, NEFT, etc.)
2. Cyber security incident such Distributed Denial of Service (DDOS), Ransomware/ cryptoware. Data breach, data destruction, web defacement, etc.
3. Unauthorised access, disclosure, tampering or theft of banks and customers" information (personal Identifiable Information and financial data).

Asignificant financial loss is a loss that exceeds 0.01% of shareholders" funds unimpaired bylosses.

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 evaluation 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 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

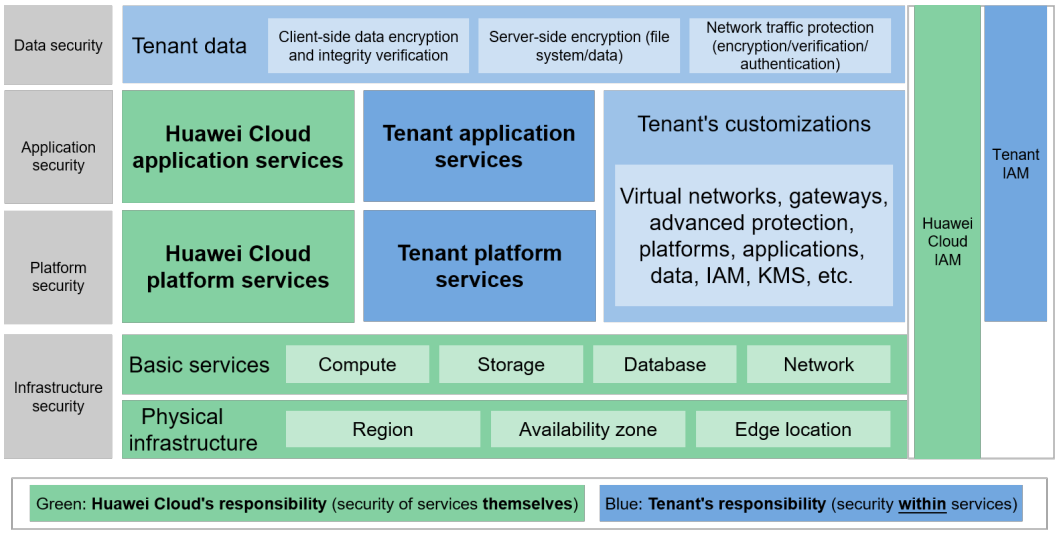
TISAX (Europe)	TISAX (Trusted Information Security Assessment Exchange) is a security standard for information security assessment and data exchange in the automotive industry launched by the Verband der Automobilindustrie (VDA) and the European Automobile Industry Security Data Exchange Association (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 - 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 tenant and HUAWEI CLOUD. As a result, HUAWEI CLOUD proposes a responsibility sharing model to help tenants 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 tenant and HUAWEI CLOUD:

Responsibility Sharing Model



As shown in the above model, the privacy protection responsibilities are distributed between HUAWEI CLOUD and tenants 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.

Tenant: The primary responsibilities of the tenants are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a tenant 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 tenant deploys on HUAWEI CLOUD. At the same time, the tenant 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 **White Paper for HUAWEI CLOUD Data Security** released by HUAWEI CLOUD.

4 HUAWEI CLOUD Global Infrastructure

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

5 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of Nigeria Financial Services Industry IT Standars Blueprint

The CBN released the Blueprint for Information Technology Standards in the Nigerian Financial Services Sector (the "Blueprint") in July 2019. This Blueprint aims to help Nigerian financial services institutions develop capabilities under eight (8) key technology Capabilities areas, including Strategic IT Alignment, IT Governance, Architecture & Information Management, Solutions Delivery, Service Management & Operations, Information & Technology Security, Workforce & Resource Management, and IT Innovation. Skills in these capability areas will support the transformation of the Financial Institutions' IT function to high performing IT operations.

When FIs are seeking to comply with the requirements stipulated in Blueprint, HUAWEI CLOUD, as a cloud service provider, may be involved in some activities that are prescribed under such requirements. The following contents summarize the requirements related to cloud service providers in Blueprint, 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

4.1	Considerations for IT Service Provider/ Vendor Engagement	This section of the Blueprint provides guidelines for ensuring due care and diligence while engaging service providers: 1. Policies and Procedures: Develop policies on vendor/ service provider engagement. Most Financial Institutions already have policies guiding interactions with contractors, vendors and service providers. This may already exist via the Financial Institution's business policies, or through the implementation of IT Standards like ITIL, ISO 20000, COBIT and /or ISO 27001. CIOs are expected to conform to these policies where they exist and also ensure that they are aligned to the Financial Institution's IT Strategy. Where there is a misalignment or where the policy that exist does not address all the concerns for IT vendors, an addendum to the existing policy is recommended.	When working with service providers, FIs should develop and implement service provider engagement policies, and CIO should ensure that engagement policies are aligned with IT strategy. HUAWEI CLOUD follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the operation of the system and rectify them to continuously improve the management system.

		2. Risk Assessment: Conduct risk assessment to understand the implications of outsourcing a task or activity to vendors/service provider Financial institutions are encouraged to conduct a risk assessment of the business activity to be performed by the vendor and determine the implications of performing the activity in-house or having the activity performed by a service provider. The benefits, risks and cost implications which are a result of such an assessment are fundamental to deciding whether to perform an activity in-house, get a vendor to perform it in-house or outsource it to be performed from the service provider’s location.	FIs should conduct a risk assessment to understand the impact of outsourcing tasks or activities to service providers. HUAWEI CLOUD as a cloud service provider, receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with risk assessment activities initiated by customers. HUAWEI CLOUD inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company.

		3. Vendor Selection: Exercise due diligence in the selection of vendors/service providers It is important that due diligence is exercised before a service provider is formally engaged. Activities recommended include: checking the service provider’s background and reputation, policies, operations and internal controls, Financial performance, and business continuity /contingency plans (where applicable). Financial Institutions are advised to independently validate and verify any certificates from certificate issuing authorities on the authenticity of the certificates presented by the vendors.	When selecting a service provider, FIs should conduct due diligence covering background and reputation, policies, operations and internal controls, financial performance, business continuity/contingency plans, service qualifications, etc. As a cloud service provider, HUAWEI CLOUD's background and reputation, policies, operations and internal controls, and financial performance are as follows: （1）background and 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 difference Chinese industries such as the internet, live on demand, video surveillance, genetics, automobile manufacturing and other industries. In overseas markets, HUAWEI CLOUD services have been launched in Hong Kong, Russia, Thailand, South Africa and Singapore. 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. (2) Policies: 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. (3) Operational: HUAWEI CLOUD follows ISO 27001, ISO 20000, ISO 22301 and other international standards to establish a sound information security management system, IT service management system, business continuity management system, and daily operation of the system applicable requirements. HUAWEI CLOUD regularly carries out risk assessment, management review, and other activities every year to identify problems in the

			operation of the system and rectify (4)Internal Controls: HUAWEI CLOUD inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company. (5) Financial Performance: 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. According to the *Market Share: IT Services, worldwide 2021* released by Gartner, HUAWEI CLOUD ranked fifth in the global IaaS market and top four in Asia Pacific. (6) Business Continuity / Contingency Plans: To provide continuous and stable cloud services to customers, HUAWEI CLOUD has established a set of complete business continuity management systems in accordance with *ISO 22301 Business Continuity Management International standards*. 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. HUAWEI CLOUD has formulated a complete contingency plan, which specifies the organization, procedures and operational specification of contingency response in detail, and carries out regular testing to ensure the continuous operation of cloud services and the business and data security of customers （7）Service Qualifications: Huawei Cloud has various certifications to ensure the security and compatible operation of its services, which include ISO27001, ISO27017, ISO27018, CSASTAR, PCIDSS, and other certifications. For more certification information, please refer to this document. 2. If necessary, financial institutions can apply to Huawei Cloud through official channels to obtain certificates as well as copies of audit reports.

		Cloud: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors – ISO 27018 Information Security Management Systems — Requirements - ISO 27001	HUAWEI CLOUD has obtained multiple certifications in relation to privacy compliance international standard, including ISO 27701, ISO 29151, ISO 27018, BS 10012, SOC privacy principles audit reports, etc. Among all the international standards, ISO27018 is the international code of conduct focusing on the privacy protection regarding cloud, its adoption indicates that HUAWEI CLOUD has a complete privacy protection management system. HUAWEI CLOUD has built a comprehensive information security management system based on ISO27001, passed the certification. and formulated the overall information security strategy of HUAWEI CLOUD. It clarified the structure and responsibilities of information security management organization, the management methods of information security system files, and the key focus areas and objectives of information security, including asset security, access control, cryptography, physical security, operational security, communication security, system development security, supplier management, information security incident management, and business continuity. HUAWEI CLOUD protects the confidentiality, integrity, and availability of customer systems and data in one comprehensive effort.

		4. Contracting: Implement thorough and rigorous contracting procedures. The contract with the vendor/ service provider must be drawn up in conjunction with and reviewed by the Financial Institution’s legal department. All contracts should contain at the minimum: i. Scope of services to be provided ii. Service performance requirements iii. Division and agreement of responsibilities iv. Contact points, communication and reporting frequency and content v. Training of Financial institution employees vi. Contract review and dispute resolution processes vii. Price structure and payment terms viii. Compliance with applicable laws, regulations, regulatory guidance and Standards ix. Intellectual property rights and copyright x. Right to audit: Contracts should contain the right of the Financial Institution or its representatives to audit the service provider and/or to have access to audit reports xi. Liability limitations xii. The ability to subcontract services xiii. Termination rights of each party xiv. Obligations at termination and beyond	Contracts between FIs and vendors/service providers must be drafted with and reviewed by the financial institution's legal department. To meet regulatory requirements in conjunction with clients, 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. HUAWEI CLOUD has also developed an online contract template, which can be customized according to the needs of different customers. Customers' and their regulators' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the actual situation.

6 How HUAWEI CLOUD Meets and Assists Customers to Meet the Requirements of Risk-based Cybersecurity Framework and Guidelines For Deposit Money Banks and Payment Service Providers, and Draft Risk-based Cybersecurity Framework and Guidelines For Other Financial Institutions (OFIs)

6.1 Cybersecurity Risk Management System and Cybersecurity Resilience Assessment

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response

DBM and PSP Guidelines 3.7、3.8	Cybersecurity Risk Management System	3.7. A DMB/PSP shall ensure consistent conduct of risk assessments, vulnerability assessments and threat analysis to detect and evaluate risk to the DMB/ PSP"s information assets and determine the appropriateness of security controls in managing risk. 3.8. IT risk shall be responsible for assessment, measurement and monitoring/reporting of risks associated with critical IT infrastructure while information/cybersecurity team shall be responsible for risk mitigation/ treatment.	FIs should develop a network security risk assessment mechanism, conduct a risk assessment, vulnerability assessments and threat analysis to detect and evaluate risk to the information assets and determine the appropriateness of security controls in managing risk. HUAWEI CLOUD, as a cloud service provider, receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with risk assessment activities initiated by customers. HUAWEI CLOUD inherits Huawei's risk management ability and establishes a complete risk management system. Through the continuous operation of the risk management system, HUAWEI CLOUD can effectively control risks in the complex internal and external environment with the huge uncertainties in the market, strive for the optimal balance between performance growth and risk, continuously manage internal and external risks, and ensure the sustainable and healthy development of the company.
Draft OFI Guidelines 3.7、3.8	Cybersecurity Risk Management System	3.7 An OFI shall regularly conduct risk assessments, vulnerability assessments and threat analysis to detect and evaluate risk to the OFI’s information assets and determine the appropriateness of security controls in managing risk. 3.8 1he IT team shall be responsible for assessment, measurement and monitoring/reporting of risks associated with critical IT infrastructure while information security/ cybersecurity team shall be responsible for risk mitigation/treatment.	

DBM and PSP Guidelines 3.9	Cybersecurity Risk Management System	3.9.1. Determining the Current Cybersecurity Profile (“present state”) 3.9.1.1. DMBs and PSPs shall determine their “current” cybersecurity position at regular intervals by evaluating all identifiable cybersecurity vulnerabilities; threats and likelihood of successful exploit; potential impact (reputational, financial, regulatory, etc.); and the associated risks in order to estimate the amount of assets and efforts required to recover from losses/damage attributable to potential cyber incidents. 3.9.1.2. The assessment should include but not limited to adequacy of cybersecurity governance; policies, procedures and standards; inherent risks in business operations; visibility to emerging threats to information assets; capability to swiftly respond and recover from cyber-incidents; vendor risk, and efficacy of existing controls to mitigate the identified risks.	FIs should assess all identifiable cybersecurity vulnerabilities, threats and likelihood of successful exploit, potential impact (reputational, financial, regulatory, etc.) and associated risks, which should include but not be limited to cybersecurity governance, inherent risks, rapid response, effectiveness of controls, etc., and all gaps identified by the assessment should be documented and communicated to senior management and the board. HUAWEI CLOUD as a cloud service provider: (1) To cooperate with customers to meet regulatory requirements, HUAWEI CLOUD provides **Host Security Service (HSS)** To help customers manage their network security status. HSS is a security manager for servers. It provides asset management, vulnerability management, baseline check, and intrusion detection functions to help enterprises better manage host security risks, detect and prevent hacker intrusion in real time. (2) HUAWEI CLOUD Event Response and Recovery Capability: The Huawei Product Security Incident Response Team (PSIRT) has a reasonably mature vulnerability response program. Considering HUAWEI CLOUD's self-service model, the program ensures rapid patching of vulnerabilities found on in-house-developed and third party technologies for HUAWEI CLOUD infrastructures, platforms,

Draft OFI Guidelines 4.1	Cybersecurity Resilience Assessment	4.1 Determining the Current Cybersecurity Profile (“present state”) 4.1.1. OFIs shall determine their “current” cybersecurity position at regular intervals by evaluating all identifiable cybersecurity vulnerabilities; threats and likelihood of successful exploit; potential impact (reputational, financial, regulatory, etc.); and the associated risks in order to estimate the amount of resources and efforts required to recover from losses/damage attributable to potential cyber incidents. 4.1.2. The assessment should include but not limited to adequacy of cybersecurity governance; policies, procedures and standards; inherent risks in business operations; visibility to emerging threats to information assets; capability to swiftly respond and recover from cyber-incidents; vendor risk, and efficacy of existing controls to mitigate the identified risks.	applications and cloud services, and reduces the risk of impact on user business operations through continuously optimizing the security vulnerability management process and technical means. 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 make 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 customers.

6.2 Cybersecurity Operational Resilience

6.2.1 Know Your Environment

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response

DBM and PSP Guidelines 4.1	Know Your Environment	4.1 Know Your Environment: A DMB/PSP shall endeavor to be acquainted with its business environment and critical assets. It shall devise mechanisms to maintain an up-to-date inventory of authorized software, hardware (workstation, servers, network devices etc.), other network devices, and internal and external network connections. All unauthorized software and hardware device on its network shall also be identified, documented, removed and reported appropriately. Employees and contractors providing information technology and cybersecurity functions/ services shall also be identified. Details on how to improve DMB/PSP"s IT infrastructure awareness is contained in Appendix III.	FIs shall endeavor to be acquainted with its business environment and critical assets, and maintain an up-to-date inventory containing all unauthorized software and hardware properly identified, recorded, removed, and reported. As a cloud service provider, HUAWEI CLOUD cooperates with customers to meet regulatory requirements. Customers can manage software assets on the cloud through the asset management function of **Host Security Service (HSS)**, which includes manages and analyzes security asset information, such as accounts, ports, processes, web directories, and software.
Draft OFI Guidelines 5.1	Know Your Environment	5.1 Know Your Environment: An OFI shall endeavor to be acquainted with its business environment and critical assets. It shall devise mechanisms to maintain an up-to-date inventory of authorized software, hardware (workstation, servers, network devices etc.), other network devices, and internal and external network connections. All unauthorized software and hardware devices on its network shall be identified, documented, removed and reported appropriately.	

DBM and PSP Guidelines Appendix III 3	Know Your Environment	3. Vendor/Contractors/ Third-parties: A DMB/PSP shall: 3.1 Maintain an up-to-date inventory of services rendered by vendor/ contractor/third-parties with valid Service Level Agreement (SLA). 3.2 Ensure that each SLA contains at minimum: details of service rendered, Non-Disclosure Agreement (NDA), Roles and Responsibilities of each party, Duration, Vendor Service Level Manager, Service Quality metric/ evaluation criteria, and the Right to Audit clause. 3.3 Audit their vendors/ contractors/third-parties in order to ensure/enforce compliance with the SLA; and promptly identify risky parties; if possible, visit their office/ IT processing facility 3.4 Assess the qualification, skills and/or experience of vendor staff assigned to them by their vendors/ contractors/third-parties.	FIs should maintain a list of services provided by vendors/ contractors/third parties and ensure that the SLA content is complete and detailed; and assess the qualifications, skills or experience of the vendor's relevant support staff. 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. HUAWEI CLOUD has also developed an online contract template, which can be customized according to the needs of different customers. Customers' and their regulators' audit and supervision rights in HUAWEI CLOUD will be committed in the agreement signed with the customer according to the actual situation. Consistent with that of the entire company, the HR management framework for HUAWEI CLOUD security personnel has been long established on the basis of applicable laws. Cloud security requires HR to ensure that our staff's backgrounds and qualifications meet the requirements of HUAWEI CLOUD services. The behavior of each HUAWEI CLOUD employee must comply with applicable laws, policies, and processes, as well as the Huawei Business Conduct Guidelines (BCG). HUAWEI CLOUD employees must consistently demonstrate the required knowledge, skills, and experience.

Draft OFI Guidelines Appendix II 3	Know Your Environment	3.3 Vendor/Contractors/ Third-parties: An OFI shall: 3.1 Maintain an up-to-date inventory of services rendered by vendor/ contractor/third-parties with valid service Level Agreement (SLA). 3.2 Ensure that each SLA contains at minimum, details of service rendered, Non-Disclosure Agreement (NDA), Roles and Responsibilities of each party, Duration, Vendor Service Level Manager, Service Quality metric/ evaluation criteria, and the Right to Audit clause. 3.3 Audit their vendors/ contractors/third-parties in order to ensure/enforce compliance with the SLA; and promptly identify risky parties; if possible, visit their office/ IT processing facility. 3.4 Assess the qualification, skills and/or experience of vendor staff assigned to them by their vendors/ contractors/third-parties.	HUAWEI CLOUD as a cloud service provider, receives regular audits from professional third-party auditing institutions every year and provides professional assistance to actively respond to and cooperate with audit requests and due diligence initiated by the customer.

DBM and PSP Guidelines Appendix III 4	Know Your Environment	4. External Connection: A DMB/PSP shall: 4.1 Identify and document all connections to third-parties -wholesale customers, vendors and switches that provide Value Added Service (VAS) -; the objective of each connection shall be documented and reviewed regularly. 4.2 Assess, document, and mitigate all risks associated with the identified external connections appropriately. 4.3 Where applicable, visit the data center and network infrastructure facilities of third-parties; access their approved cybersecurity policies and ensure it addresses all cybersecurity concerns. 4.4 Ensure that third-party accesses are restricted to only authorized segment of the network; only specific IP addresses from the third-party shall be allowed, and restrict connection(s) to a period of time (where applicable). 4.5 Always log, monitor, and review all third-party connections to their network.	FIs shall identify and record all connections to third parties, manage authorization of third-party access, ensure that third-party access is limited to authorized segments of the network, and review it periodically. HUAWEI CLOUD provides **Cloud Trace Service (CTS)** to keep track of user operations and resource changes on your cloud resources. CTS helps you collect, store, and query operational records for security analysis, audit and compliance, and fault location. HUAWEI CLOUD facilitates data isolation in the cloud through the Virtual Private Cloud (VPC) service, the VPC uses the network isolation technology to isolate tenants at Layer 3. Tenants can control their own virtual network construction and configuration. On the one hand, a tenant's VPC can be connected to the tenant's enterprise network traditional data center using VPN or Direct Connect service such that tenant's applications and data residing in its internal network can be seamlessly migrated to the tenant's VPC. On the other hand, the ACL and security group function of the VPC can be used to configure network security and access rules as per the tenant's specific requirements for finer-grained network segregation. In terms of network border protection, HUAWEI CLOUD has established a solid and complete border and multi-layer security protection

Draft OFI Guidelines Appendix II4	Know Your Environment	4. External Connection: An OFI shall: 4.1 Identify and document all connections to third-parties -wholesale customers, vendors and switches that provide Value Added Service (VAS) the objective of each connection shall be documented and reviewed regularly. 4.2 Assess, document, and mitigate all risks associated with the identified external connections appropriately. 4.3 Where applicable, visit the data center and network infrastructure facilities of third-parties; access their approved cybersecurity policies and ensure it addresses all cybersecurity concerns. 4.4 Ensure that third-party accesses are restricted to only authorized segment of the network; only specific IP addresses from the third-party shall be allowed, and restrict connection(s) to a period of time (where applicable). 4.5 Always log. monitor, and review all third-party connections to their network.	system, and deployed Anti-DDoS, IDS/IPS, and WAF protection mechanisms. Anti-DDoS quickly detects and defends against DDoS attacks and comprehensively defends against traffic attacks and application-layer attacks in real time. WAF detects and defends against web attacks in real time, generates alarms for high-risk attacks, and blocks them immediately. The IDS/IPS detects and blocks network attacks from the Internet in real time and monitors abnormal host behaviors.

6.2.2 Enhancing Cybersecurity Resilience

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response

DBM and PSP Guidelines Appendix IV 1	Enhancing Cybersecurity Resilience	1. Access Control: A DMB/PSP shall establish an access control policy which ensures that: a. There exists mechanism, standards and procedures that govern users, systems and service accounts access provisioning, identification, and authorization to all systems, network, and applications. b. All workstations/laptops, end-users, service accounts, network devices (internal and external), and administrators have identities and credentials to access the bank's resources. c. Access to its information assets (including customer information), resources and connected services/facilities at any time are limited to only authorize users, services, processes or devices (including wireless network) based on the principle of least privilege and guided by an access control matrix. d. Authorizations given to users, service and system accounts are limited to the functions/ services they provide; where necessary implement logon time and days restriction. e. Physical access to assets is controlled based on the criticality and sensitivity of the information processed, stored and transmitted by them. f. The repositories of all users, administrator, and system identities and credentials are protected.	FIs shall establish access control policies, set user rights that match their responsibilities, adopt secure authentication and data encryption technologies, and record user access through logs. As a cloud service provider, HUAWEI CLOUD, to cooperate with customers to meet regulatory requirements: (1) Customers can manage user accounts using cloud resources through HUAWEI CLOUD **Identity and Access Management (IAM)**. Each HUAWEI CLOUD customer has a unique user ID in HUAWEI CLOUD. In addition, HUAWEI CLOUD provides a variety of user authentication mechanisms. 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. (2) HUAWEI CLOUD encrypts customers' personal data to ensure its security during storage and transmission. By default, cloud services encrypt customers' sensitive personal data (if any) and all data transmitted over untrusted networks. At the same time, HUAWEI CLOUD provides **Database Security Service (DBSS)**, which can be used for security protection of the database of personal data storage, includes two functional modules: database security audit and database security

Draft OFI Guidelines Appendix III 1	Enhancing Cybersecurity Resilience	1. Access Control: An OFI shall establish an access control policy which ensures that: a. There exists mechanism, standards and procedures that govern users, systems and service accounts access provisioning, identification, and authorization to all systems, network, and applications. b. All workstations/laptops, end-users, sendee accounts, network devices (internal and external), and administrators have identities and credentials to access the bank's resources. c. Access to its information assets (including customer information), resources and connected services/facilities at any time are limited to only authorize users, services, processes or devices (including wireless network) based on the principle of least privilege and guided by an access control matrix. d. Authorizations given to users, service and system accounts are limited to the functions/services they provide; where necessary implement logon time and days restriction. e. Physical access to assets is controlled based on the criticality and sensitivity of the information processed, stored and transmitted by them. f. The repositories of all users, administrator, and system identities and credentials are protected.	protection. It provides three functions: database audit, data leakage prevention, and database firewall ensuring database and asset security on the cloud.

DBM and PSP Guidelines Appendix IV 2	Enhancing Cybersecurity Resilience	2. Secure System Configuration Management: To enhance resilience through system configuration, a DMB/PSP shall: a. Acquire and deploy systems/applications with in-built resilience configuration. b. Develop minimum security baseline configuration such as anti-malware; data loss prevention solutions; and systems security settings for workstations/laptops, servers, applications/ software including network devices governed by vendor recommendations, informative references in Appendix V and the CBN guidelines. c. Devise mechanisms to logically apply and maintain their cybersecurity policies and security baseline configuration on systems, applications and network devices. d. Establish a Standard Operating Procedures (SOP) for all IT processes and activities. e. Audit the security configurations items on system and network devices to ensure compliance with preconfigured security settings. f. Devise a mechanism to monitor, detect, log and report all unauthorized system configuration changes; where possible, the mechanism shall re-apply the security configuration seamlessly.	FIs shall establish a minimum security baseline configuration and monitor, monitor, log and report all unauthorized system configuration changes FIs can perform baseline checks, monitor for malicious programs, etc. through the **Host Security Service (HSS).** HSS is a security manager for servers. It provides asset management, vulnerability management, baseline check, and intrusion detection functions to help enterprises better manage host security risks, detect and prevent hacker intrusion in real time, or check and configure the security baseline of the Cloud Service using the HUAWEI CLOUD Security Baseline Configuration Guide. HUAWEI CLOUD provides **Cloud Trace Service (CTS)** to keep track of user operations and resource changes on your cloud resources. CTS helps you collect, store, and query operational records for security analysis, audit and compliance, and fault location.

Draft OFI Guidelines Appendix III 2	Enhancing Cybersecurity Resilience	2. Secure System Configuration Management: To enhance resilience through system configuration, an OFI shall: a. Acquire and deploy systems/applications with in-built resilience configuration. b. Develop minimum security baseline configuration such as anti-malware; data loss prevention solutions; and systems security settings for workstations/laptops, servers, applications/ software including network devices governed by vendor recommendations, informative references in Appendix IV and the CBN guidelines. c. Devise mechanisms to logically apply and maintain their cybersecurity policies and security baseline configuration on systems, applications and network devices. d. Establish a Standard Operating Procedures (SOP) for all IT processes and activities. e. Audit the security configurations items on system and network devices to ensure compliance with preconfigured security settings. f. Devise a mechanism to monitor, detect, log and report all unauthorized system configuration changes; where possible, the mechanism shall re-apply the security configuration seamlessly.	

DBM and PSP Guidelines Appendix IV 4	Enhancing Cybersecurity Resilience	4. Data Loss Prevention: Protecting and controlling the accessibility and usage of customers Personal Identifiable Information (PII) and bank's sensitive and critical information within and outside the corporate network is a major goal of cybersecurity resilience. Hence, a. A DMB/PSP shall develop a data loss/leakage prevention strategy to discover, monitor, and protect sensitive and confidential business and customer data/information at endpoints, storage, network, and other digital stores, whether online or offline. b. The strategy should provide but not limited to a mechanism that: i. classifies both structured and unstructured data/ information; ii. discovers where sensitive/ confidential data/ information are stored; iii. monitors how sensitive/ confidential data/ information are being used; iv. continuously protects data whether the endpoint is on/off the corporate network; v. addresses notable data loss concerns through USB, e-mail, mobile phones and web; vi. takes prompt actions when a potential data breach is suspected or detected: e.g. blocking an employee's attempt to save a sensitive information to an	FIs shall develop a data loss prevention strategy, including a data classification strategy, a data identification and monitoring strategy, a data migration strategy, an asset destruction strategy, and verify that the vendor has a similar strategy. The tenant always owns and has full control of its data no matter which HUAWEI CLOUD service it subscribes to. The tenant is responsible for security configuration that are necessary to ensure its data confidentiality, integrity, availability as well as identify authentication and authorization for data access. HUAWEI CLOUD provides **Data Security Center (DSC)**, DSC is a new-generation cloud-native data security platform that provides basic data security capabilities which helps identify, classify, and mask sensitive or confidential data Customers can use DSC to integrate the status of each phase of the data security lifecycle to build a cloud service panorama to protect the security of data collection, storage, transmission, use, exchange, and destruction And HUAWEI CLOUD provides **Database Security Service (DBSS)** uses machine learning mechanism and big data technologies to protect customers' databases on the cloud, audit and detect risky behaviors, such as SQL injection, operational risks identification etc. Customers can use DBSS to detect potential risks and ensure the security of their databases.

		external storage or network share drive; and vii. establishes to management a reduction in data loss risk in institution. c. Critical and sensitive information on assets shall be formally managed throughout removal, transfers, and disposition. All assets identified for disposal shall undergo degaussing, and/or total destruction; in accordance with its approved policy. d. A DMB/PSP shall validate that similar control exist at vendor managed facilities such as co-location data centers, and cloud service providers.	HUAWEI CLOUD attaches great importance to the security of users' data and information assets, and its security strategy and policy include a strong focus on data protection. HUAWEI CLOUD will continue to embrace industry-leading standards for data security lifecycle management and adopt best-of-breed security technologies, practices, and processes across a variety of aspects, including identity authentication, privilege management, access control, data isolation, transmission, storage, deletion, and physical destruction of storage media. In short, HUAWEI CLOUD will always strive toward the most practical data protection capabilities in order to safeguard the privacy, ownership, and control of ourtenants' data against data breaches and impacts on their business. HUAWEI CLOUD uses multiple privacy protection tools to help HUAWEI CLOUD quickly, systematically, and efficiently manage privacy protection. **Data discovery and management:** The data discovery tool can identify personal data in systems, databases, or files checking whether a business activity contains personal data and the type and transfer status of the data. The tool can also help users take appropriate privacy protection measures. Data Administration Service (DAS) helps HUAWEI CLOUD register and manage data assets throughout their lifecycle.

Draft OFI Guidelines 4.1	Enhancing Cybersecurity Resilience	4. Data Loss Prevention: Protecting and controlling the accessibility and usage of sensitive and critical information within and outside the corporate network is a major goal of cybersecurity resilience. Hence, a. an OFl shall develop a data loss/leakage prevention strategy to discover, monitor, and protect sensitive and confidential business and customer data/information at endpoints, storage, network, and other digital stores, whether online or offline. b. The strategy should provide but not limited to a mechanism that: i. classifies both structured and unstructured data/ information; ii. discovers where sensitive/ confidential data/ information are stored; iii. monitors how sensitive/ confidential data/ information are being used; iv. continuously protects data whether the endpoint is on/off the corporate network; v. addresses notable data loss concerns through USB, e-mail, mobile phones and web; vi. takes prompt actions when a potential data breach is suspected or detected: educate employees through a warning pop-up message, encryption, or prevent the action; and	**Privacy risk analysis:** The risk analysis process can be implemented using a range of tools, helping business teams identify privacy protection risks and develop and take countermeasures. **Encrypted Data Leakage Prevention:** HUAWEI CLOUD encrypts customers' personal data to ensure its security during storage and transmission **Data deletion:** HUAWEI CLOUD has developed a media management process to ensure the security of the data stored in the media. If customers want to delete data or data needs to be deleted due to the expiration of a service, HUAWEI CLOUD will strictly follow applicable laws and regulations，as well as agreements with customers, delete the stored customer data in accordance with data destruction standards. This is achieved as follows: 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 so the 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 so that data on the storage medium cannot be restored. **Internal Management:** In order to ensure the security and stable operation of Huawei's cloud platform and

		vii. establishes to management a reduction in data loss risk in institution c. Critical and sensitive information on assets shall be formally managed throughout removal, transfers, and disposition. All assets identified for disposal shall undergo degaussing, and/or total destruction; in accordance with its approved policy. d. An OFI shall validate that similar control exist at vendor managed facilities such as co-location data centers, and cloud service providers.	network, HUAWEI CLOUD has adopted a series of management measures, including: vulnerability analysis and processing, log monitoring, incident response, optimization of the default security configuration of cloud products, security patch deployment, antivirus software deployment, regular backup of system and device profiles and testing of backup effectiveness

DBM and PSP Guidelines Appendix IV 5	Enhancing Cybersecurity Resilience	5. System Life Cycle Management: In managing the life cycle of systems, a DMB/PSP shall: a. Establish policies and procedures that consistently oversee the lifecycle (identification, acquisition/ development, maintenance/ update, and disposal) of applications, components, and systems. b. Ensure that cybersecurity control are considered and incorporated in all stages of the system/application lifecycle. The business requirement for the acquisition/development of systems/applications shall also identify and document the security requirements. This includes but not limited to access control, access right management, authentication, event logging, audit trail, user session management, separation of duties, and least privilege, etc. aration of duties, and least privilege, etc. c. Validate that the systems/ applications meet all other requirements (functional, performance, reliability, etc.) and any applicable CBN regulations before they are deployed. d. Ensure that all in-house applications are developed in-line with secure coding practices such as threat modeling, input validation, least privilege, defense in-depth, and fail secure whilst mitigating against OWASP vulnerabilities. These applications shall also be thoroughly tested by a team of qualified software testers	FIs should establish policies and procedures to continuously monitor the lifecycle of applications, components, and systems and ensure that cybersecurity controls are incorporated at all stages; verify that functional, performance, reliability, or other regulatory requirements are met prior to deployment, and ensure that all internal applications are developed in compliance with secure coding practices; production, development, and test environments should be separate, access needs to be controlled, and development and test environments There should be no sensitive data in the development and test environments; data should be encrypted. As a cloud service provider: (1) HUAWEI CLOUD establish and mature its multi-faceted full-stack security protection framework and high-availability, high-reliability cloud services. And the continuous integration, delivery, and deployment practices, which are characteristic of online and cloud services development and operations, require entirely new mindset, methodologies, and processes, as well as an all-new tool chain. By leveraging Huawei's wealth of experience and far-reaching capabilities in the field of security, HUAWEI CLOUD has not only proactively pursued the new DevOps process, which features rapid and continuous iteration capabilities, but also seamlessly integrated the Huawei security development lifecycle (SDL). As a result,

		and business/application owners. e. Separate the production/ live environment from the development and testing environment(s). f. Sanitize sensitive data in the development and testing environments by implementing a Data Masking solution to mask/ fabricate bank's and customers" sensitive information for the purpose of development, System and User Acceptance Tests. g. Establish a procedure for the maintenance of on-site and remote organizational assets to prevent unauthorized access. h. Adopt cryptographic controls such as public key infrastructure, hashing and encryption to guard confidential and sensitive information against unauthorized access. i. Comply with the extant rules and regulations of your card schemes and associated stakeholder rules.	DevOps is gradually taking shape as a highly automated new security lifecycle management methodology and process, called DevSecOps, alongside cloud security engineering capabilities and tool chain that together ensure the smooth and flexible implementation of DevSecOps. (2) HUAWEI CLOUD and related cloud services comply with security and privacy design principles and specifications as well as legal and regulation requirements. For example, HUAWEI CLOUD runs threat analysis based on the service scenario, data flow diagram, and networking model during the security requirement analysis and design phases. The threat analysis library, threat mitigation library, and security design solution library used to guide HUAWEI CLOUD threat analysis draws from security accumulation and industry best practices in traditional products and new cloud domain products. After identifying the threat, design engineers develop mitigation measures by utilizing the threat mitigation library and security design solution library, and then implement the corresponding security solution design. All threat mitigation measures will eventually become security requirements and functions. Additionally, security test case design is completed in accordance with the company's security test case library, and these designs are then implemented to ensure

Draft OFI Guidelines AppendixIII5	Enhancing Cybersecurity Resilience	5. System Life Cycle Management: In managing the life cycle of systems, an OFI shall: a. Establish policies and procedures that consistently oversee the lifecycle (identification, acquisition/ development, maintenance/ update, and disposal) of applications, components, and systems. b. Ensure that cybersecurity controls are considered and incorporated in all stages of the system/application lifecycle. The business requirement for the acquisition/development of systems/applications shall also identity and document the security requirements. This includes but not limited to access control, access right management, authentication, event logging, audit trail, user session management, separation of duties, and least privilege etc. c. Validate that the systems/ applications meet all other requirements (functional, performance, reliability, etc.) and any applicable CBN regulations before they are deployed. d. Ensure that all in-house applications are developed in-line with secure coding practices such as threat modeling, input validation, least privilege, fault deny, defense in-depth, and fail secure whilst mitigating against OWASP vulnerabilities. These applications shall also be thoroughly tested by a team of independent software testers and business/ application owners. e. Separate the production/ live environment from the development/testing environment(s). f. Establish a procedure for the maintenance of on-site	the ultimate security of products and services. (3) HUAWEI CLOUD strictly complies with the secure coding specifications released by Huawei. Before they are on boarded, HUAWEI CLOUD service development and test personnel are all required to learn corresponding specification and prove they have learned these by passing examinations on them. In addition, we introduced a daily check of the static code scanning tool, with the resulting data being fed into the cloud service Continuous Integration/Continuous Deployment (CI/CD) tool chain for control and cloud service product quality assessment through the use of quality thresholds. Before any cloud product or cloud service is released, static code scanning alarm clearing must be completed, effectively reducing the code related issues that can extend rollout time coding. (4) All cloud services pass multiple security tests before release, including but not limited to micro service-level functions and interface security tests such as authentication, authorization, and session security in the alpha phase; API and protocol fuzzing type of testing incorporated in the beta phase; and database security validation testing in the gamma phase. The test cases cover the security requirements identified in the security design phase and include test cases from an attacker's perspective. In addition, HUAWEI CLOUD leverages its in-depth

			understanding of customers' security requirements and industry standards and develops matching security test tools. (5) HUAWEI CLOUD extensively uses encryption technology to encrypt customer personal data for storage and transmission, ensuring security in the storage and transmission of personal data. Huawei Cloud recommends that tenants encrypt and store important data to be uploaded to the cloud to prevent leakage. When data needs to be deleted, it is prevented from being leaked after being restored to plaintext before being completely deleted by directly deleting the relevant data encryption key. HUAWEI CLOUD provides **Data Encryption Workshop (DEW)**, DEW is a comprehensive cloud data encryption service. It provides functions such as dedicated encryption, key management, and key pair management. It uses HSMs to protect the security of keys. DEW can be integrated with other HUAWEI CLOUD services to meet your needs for various encryption scenarios. Users can also use this service to develop their own encryption applications. Without authorization, no one except the customers can obtain keys to decrypt data, which supports data security on the cloud.

DBM and PSP Guidelines Appendix IV 6	Enhancing Cybersecurity Resilience	6. Vulnerability Management: IT vulnerability management is an integral part risk management. To this end, a DMB/PSP shall promptly identify weaknesses in their IT infrastructure (database, applications, network etc.), account profiles (system administrators and privileged users), vendors, etc. a. Information Assets: To promptly identify all system vulnerabilities and cybersecurity risks to operations and IT assets, a DMB/PSP shall: i. Implement a vulnerability management policy; approved by Executive Management ii. Establish an automated mechanism to detect all vulnerabilities in its assets. This includes but not limited to workstations, network devices, servers (production, test and development), etc. The vulnerabilities and threats shall be documented; potential business impact and likelihood shall also be identified. iii. Conduct vulnerability assessment at least quarterly or when there is a significant change (such as installation of new systems, devices, applications, etc.) to the bank's information processing infrastructure or when vulnerabilities are made known. iv. Further identify vulnerabilities in their assets by engaging professionals in	FIs shall develop and implement a vulnerability management policy, establish an automated mechanism to continuously monitor, analyze and assess, and document vulnerabilities, and classify and resolve them according to their level as well as risk level until they are closed. FIs shall hire cybersecurity professionals to conduct penetration tests annually; and shall develop a security patch management process. HUAWEI CLOUD provides **Vulnerability Scan Service (VSS)**, VSS is a multi-dimensional security detection service with five core functions: Web vulnerability scanning, operating system vulnerability scanning, asset content compliance detection, configuration baseline scanning, and weak password detection. Customers can use VSS to automatically identify security threats to websites or servers exposed to the network, thereby protecting the integrity of data. Also，HUAWEI CLOUD provides **Situation Awareness (SA)** that helps customers manage vulnerabilities by obtaining real-time information on industry hot security vulnerabilities, synchronizing host vulnerability scans and website vulnerability scans, fully grasping the vulnerability risk status of assets on the cloud, and providing corresponding vulnerability repair recommendations. Combined with big data analysis, highly accurate threat intelligence database, "real-time monitoring" of

		this field to conduct Penetration Tests (PT) annually. However, PT shall be conducted frequently on internet-facing systems/ applications. v. Continuously identify the inherent risks and vulnerabilities associated with IT platform/protocols used for business services e.g. USSD and SMS mobile Banking protocols. vi. Promptly categorize and resolve issues identified during vulnerability assessment based on their criticality, likelihood and impact. Subsequent validation to assess closure of such vulnerabilities shall also be done. The root cause of the identified vulnerabilities such as a flaw in security policy, system misconfiguration, inconsistent Standard Operating Procedure (SOP), non-compliance to change management processes, and superficial risk assessment shall also be addressed to thwart future occurrence. vii. Have a dedicated team that monitors the release of security patches/updates by their vendors / OEMs. Security updates are mandatory, and shall be deployed quickly in accordance with DMBs and PSPs" patch management policy. Patches for well-known or zero day vulnerabilities shall also be applied swiftly in accordance with its emergency patch management process. viii. Establish an efficient mechanism and processes to	threats on the cloud, analysis of threat attacks, timely provision of alert notifications, and pre-set response strategies for typical threat events. HUAWEI CLOUD as a cloud service provider： The Huawei Product Security Incident Response Team (PSIRT) has a reasonably mature vulnerability response program. The nature of HUAWIE 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 HUAWIE CLOUD infrastructure, IaaS, PaaS and SaaS services, mitigating risks to tenants' business operations. In addition, Huawei PSIRT and HUAWIE CLOUD's security O&M team have established a mature and comprehensive program and framework for vulnerability detection, response, and disclosure. HUAWIE CLOUD relies on this program and framework to manage vulnerabilities and ensure that vulnerabilities in HUAWIE 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. HUAWIE CLOUD strives to reduce and ultimately prevent vulnerability exploitation related service impacts to our customers.

		identify assets patch compliance status - on operating system and application software on users" laptops and desktop, servers (including those on the DMZ), virtual machines, etc. - and remedy patch deficiencies.	HUAWEI CLOUD has set up an end-to-end vulnerability response work order system covering every step of the process, from vulnerability detection, identification to hotfix and patch management. This system automatically collects vulnerabilities from various channels such as PSIRT and online scanning tools, and then automatically assigns priority ratings based on criticality and maps with vulnerability resolution SLAs. In the case of a major vulnerability, the security O&M team uses in-house tools to scan HUAWEI CLOUD network, maps out the scope of affected services, systems and components within minutes. In addition, the security O&M team takes necessary vulnerability mitigation measures based on the live network situation, for example, restricting port access and implementing WAF vulnerability rules to protect or isolate effective services, reducing the risk of vulnerability exploitation. Canary deployment or blue-green deployment is used when vulnerabilities are fixed through a patch or version to minimize the impact on tenant services. In addition, HUAWEI CLOUD continuously updates operating system and container images, and rectifies system vulnerabilities by rolling upgrade of the images and containers. This does not affect tenant services.

Draft OFI Guidelines Appendix III 6	Enhancing Cybersecurity Resilience	6. Vulnerability Management: AN OFI shall promptly identify latent weaknesses in their IT infrastructure (assets), account profiles (system administrators and privileged users), and vendors. a. Information Assets: To promptly identify all system vulnerabilities and cybersecurity risks to operations and IT assets, an OFI shall: i. Implement a vulnerability management strategy; approved by the Board of Directors, ii. Establish an automated mechanism to detect all vulnerabilities in its assets. This includes but not limited to workstations, network devices, servers (production, test and development), etc. The vulnerabilities and threats shall be documented: potential business impact and likelihood shall also be identified. iii. Conduct vulnerability assessment at least quarterly or when there is a significant change (such as installation of new systems, devices, applications etc.) to the bank's information processing infrastructure or when vulnerabilities are made known. iv. Further identify vulnerabilities in their assets by engaging professionals in this field to conduct Penetration Tests (PT). The PT shall be conducted frequently on internet facing systems/applications.	

		v. Continuously identify the inherent risks and vulnerabilities associated with IT platform/protocols used for business sendees e.g. USSD and SMS mobile Banking protocols vi. Promptly categorize and resolve issues identified during vulnerability assessment based on their criticality, likelihood and impact. Subsequent validation to assess closure of such vulnerabilities shall also be done. The sources of the identified vulnerabilities such as a flaw in security policy, system misconfiguration, inconsistent Standard Operating Procedure (SOP), non-compliance to change management processes, and superficial risk assessment shall also be addressed to thwart future occurrence. vii. Have a dedicated team that incessantly monitors the release of security patches/updates by their vendors / OEMs. Security updates are mandatory, and shall be deployed quickly in accordance with DMBs and PSPs" patch management policy. Patches for well-known or zero-day vulnerabilities shall also be applied swiftly in accordance with its emergency patch management process. viii. Establish an efficient mechanism and processes to identify assets patch compliance status -on operating system and application software on users' laptops and desktop, servers (including those on	

		the DMZ), virtual machines, etc. -and remedy patch deficiencies.	

HDBM and PSP Guidelines Appendix IV 6	Enhancing Cybersecurity Resilience	b. System Administrators And Privileged Accounts: To limit exposure to insider threat, a DMB/PSP shall: i. Identify all employees and system/service accounts with super-privileges on each system, application, database, and device; and enforce segregation of duties and principle of least privilege for these accounts. ii. Where applicable, enforce password and account-management policies and practices to these accounts as-well. Use of shared default/anonymous privileged account by multiple users is highly prohibited. iii. Ensure that no single administrator have unfettered access to its critical systems. Logon credentials to critical systems, applications, and network shall be created and separately documented by at least 2 different employees. iv. Change the logon credentials of default system accounts on assets before they are connected to the network. This shall apply to test and development servers as well. v. Establish a strategy, mechanism and an intelligent procedure to log, monitor, and audit actions performed by these accounts. All logs/audit trails shall be preserved and regularly reviewed in accordance with each institution‘s account management policy.	FIs shall identify all employee and system/service accounts with super privileges on each system, application, database, and device; and implement the principles of segregation of duties and least privilege for these accounts, and audit the operation of the accounts. HUAWEI CLOUD as a cloud service provider. (1)To ensure HUAWEI CLOUD platform security, HUAWEI CLOUD has taken a minimalist approach in building an extremely stripped-down host OS and also performs security hardening on all its services. In addition, Huawei Cloud enforces stringent privilege access management (PAM) on Huawei Cloud administrators who have host OS access and enables comprehensive logging and centralized log management of all administrator level O&M activities. Huawei Cloud administrators must pass two-factor authentication in order to access the management plane through bastion hosts. All operations are logged and delivered to the centralized log audit system in time (2) With the HUAWEI CLOUD's **Identity and Access Management (IAM)**, the customer administrator can manage user accounts and control the access privileges of these user accounts. When multi-user cooperative operation resources exists in customer enterprises, IAM can avoid sharing account keys with other users, assign users minimum privileges on demand, and assist the security of user accounts by

Draft OFI Guidelines Appendix III 6	Enhancing Cybersecurity Resilience	b. System Administrators and Privileged Accounts: To limit exposure to insider threat, an OFI shall: i. Identify all employees and system/service accounts with super-privileges on each system, application, database, and device; and enforce segregation of duties and principle of least privilege for these accounts. ii. Where applicable, enforce password and account-management policies and practices to these accounts as-well. Use of shared default/anonymous privileged account by multiple users is highly prohibited. iii. Ensure that no single administrator have unfettered access to its critical systems. Logon credentials to critical systems, applications, and network shall be created and separately documented by at least 2 different employees. iv. Change the logon credentials of default system accounts on assets before they are connected to the network. This shall apply to test and development servers as well. v. Establish a strategy, mechanism and an intelligent procedure to log, monitor, and audit actions performed by these accounts. All logs/audit trails shall be preserved and regularly reviewed in accordance with each institution's account management policy.	setting a login authentication strategy, password strategy and access control list. (3) Provides **Cloud Trace Service (CTS)** for the collection, storage and query functions of various cloud resource operation records, which can be used to support common application scenarios such as security analysis, compliance audit, resource tracking and problem location.

DBM and PSP Guidelines Appendix IV 6	Enhancing Cybersecurity Resilience	c. Vendors: A DMB/PSP shall ensure that: i. No vendor has unfettered access to its systems, database, network and applications (especially the core application). ii. If a vendor needs to access its information asset, management approval shall be sought only for the duration the access is required. Such access shall be administered by an authorized administrator. iii. No vendor given logged-on to its information assets shall be left unattended to. Their actions shall be logged and closely monitored at all time. If possible, conduct a background check on all vendor staff before they are granted access.	FIs shall establish procedures for vendors to access their systems, databases, networks and applications, with access subject to approval and authorization, and monitoring when accessing. HUAWEI CLOUD, as a cloud service provider, is only a tenant data host, and the tenant has ownership and control of its data. Huawei Cloud never allows operations and maintenance operations personnel to access tenant data without authorization.
Draft OFI Guidelines Appendix III 6	Enhancing Cybersecurity Resilience	c. Vendors: An OFI shall ensure that: i. No vendor has unfettered access to its systems, database, network and applications (especially the core application). ii. If a vendor needs to access its information asset, management approval shall be sought and such access shall be administered by an authorized administrator. iii. No vendor given logged-on to its information assets shall be left unattended to. Their actions shall be logged and closely monitored at all time. If possible, conduct a background check on all vendor staff before they are granted access.	

DBM and PSP Guidelines Appendix IV 8	Enhancing Cybersecurity Resilience	7. Continuous Security Monitoring: There shall be an ongoing awareness of information security vulnerabilities and threats to support s DMB/ PSPs risk management decisions. To improve surveillance, it shall: a. Determine what needs to be monitored by: gathering information about all systems, databases, and network that support business activities; analyze reports about cyber-incidents that have occurred in the past; evaluate the recommendations from both recent internal and third-party audits/ risk assessment of the network; and report of its cybersecurity self-evaluation. c. Determine appropriate performance metrics for those variables; this includes but not limited to skills, system availability, event logging capability of systems to be monitored etc. d. Establish how the log data collected from various sources will be stored and secured. e. Define a continuous security monitoring policy/ strategy; it shall include but not limited to the identified systems and processes, key dependent variables and their performance metrics, roles and responsibilities, duration to retain log data, events that would trigger these systems to send alerts, monitoring intervals/ frequency, and how identified cyber-incidents /	FIs should develop and review disaster recovery and business continuity plan documents and adopt automatic detection tools for early detection of network events. HUAWEI CLOUD provides the following three products to help FIs continuously monitor security: (1) Host Security Service (HSS) provides asset management, vulnerability management, baseline check, and intrusion detection functions to help enterprises better manage host security risks, detect and prevent hacker intrusion in real time (2) **Situation Awareness (SA)** is HUAWEI CLOUD security management and situation analysis platform. It is capable of detecting over 20 categories of security threats on the cloud, including DDoS attacks, brute force cracking, web attacks, backdoor Trojans, zombie hosts, abnormal behavior, vulnerability attacks, command and control, and so on. Using big data analysis technology, situational awareness can classify statistics and comprehensive analysis of attack events, threat alerts and attack sources, presenting users with a global security situation. (3) **Managed Threat Detection(MTD),** by accessing the IAM logs, DNS logs, CTS logs, OBS logs, and VPC logs generated by users' operations in Huawei Cloud in the target area, the IP or domain name of visitors in the logs will be continuously detected for potential malicious activities and

		breaches will be contained, treated, documented, and reported. f. Determine a baseline of operations and expected data flows for users, systems, and network of the identified systems. This includes but not limited to logon hours, network traffic threshold, level of processor utilization, etc. g. Implement across all-delivery channels a risk-based transaction monitoring mechanism which shall securely notify customers of all payment or fund transfer transactions above a specified value defined by customers. h. Establish a non-intrusive real-time monitoring mechanism to collect, correlate, and detect anomalous user, administrator, system, and process/service activities on critical system, database, and network in a timely manner while verifying the effectiveness of protective measures in place. i. Ensure that the mechanism provides Value Added Services (VAS) such as separating real events from nonimpact events (false positive), locating and containing events, sending alerts to appropriate staff for investigation, remediation, reporting, keeping historical data for the purpose of forensics, and managing operational risks. j. Monitor the physical environment of assets – server room, network devices, data center, disaster	unauthorized behaviors, and any detected abnormality will be alerted in time. It integrates log detection models, such as AI detection engine, threat intelligence, and detection policy, to identify threats to Intelligent detection from multiple cloud services (Includes IAM service, DNS service, CTS service, OBS service, VPC service) The abnormal access behaviors implied in the log data, proactively discover potential threats, generate alert information for access behaviors that may have threats, and output alert results. Users can verify and process the alarm information through the alarm descriptions, so that potential threats can be handled and service security can be upgraded and reinforced in a timely manner before causing major losses such as information leakage, thus protecting users' account security and ensuring stable service operation. Given the professionalism and urgency to handle security incidents, HUAWEI CLOUD has a professional security incident response team available 7*24 and a corresponding pool of security expert resources for response. 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

		recovery site, and off-site storage location –to detect potential threats in a timely manner. k. Establish an effective and efficient non-intrusive mechanism to detect and perform remediation actions on malicious codes and unauthorized mobile codes on all systems (including those on the DMZ). For signature based solutions, frequency of update shall be at least daily. l. DMBs and PSPs that intends to or have cloud service providers shall be guided by the continuous security monitoring recommendation of Cloud Security Alliance (CSA).	have a serious impact on multiple customers, HUAWEI CLOUD can promptly notify customers of events with an announcement. The contents of the notification include but not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, HUAWEI CLOUD will provide the incident report to the customer according to the specific situation. HUAWEI CLOUD has established comprehensive physical security and environmental safety protection measures, strategies, and procedures. During the design, construction, and operation stages, the data centers have proper physical zoning and well-organized placement of information systems and components, which helps prevent potential physical and environmental risk scenarios (for example, fire or electro-magnetic leakage) as well as unauthorized access. Furthermore, sufficient data center space and adequate electrical, networking, and cooling capacities are reserved in order to meet not only today's infrastructure requirements but also the demands of tomorrow's rapid infrastructure expansion. The Huawei Cloud O&M team enforces stringent access control, safety measures, regular monitoring and auditing, and emergency response measures to ensure the physical security and

Draft OFI Guidelines Appendix III 7	Enhancing Cybersecurity Resilience	There shall be an ongoing awareness of information security vulnerabilities and threats to supports OFIs risk management decisions. To improve surveillance, it shall: a. Determine what needs to be monitored by: gathering information about all systems, databases, and network that support business activities; analyze reports about cyber¬ incidents that have occurred in the past; evaluate the recommendations from both recent internal and third-party audits/ risk assessment of the network; and report of its cybersecurity self-evaluation. c. Determine appropriate performance metrics for those variables; this includes but not limited to skills, system availability, event logging capability of systems to be monitored etc. d. Establish how the log data collected from various sources will be stored and secured. e. Categorize the identified systems and processes needed to be monitored according to their criticality and sensitivity to its operations. f. Define a continuous security monitoring policy/ strategy which shall be approved by the Board of Director; it shall include but not limited to the identified systems and processes, key dependent variables and their performance metrics, roles and responsibilities,	environmental safety of HUAWEI CLOUD data centers. In addition to the high availability infrastructure, data redundancy and backup, and DR among AZs, Huawei Cloud also has a formal business continuity plan (BCP) and conducts BCP drills periodically. This plan, which applies to major disasters such as earthquakes or public health crises, ensures continued operations of HUAWEI CLOUD services and safeguards customers' service and data security. HUAWEI CLOUD has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first bring the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, then, perform system operations and migration as specified in the DRP, and lastly, verify the service and business operations functions in the presumably disaster-impacted region. Test results are then annotated and archived for continuous improvement of the DRP. Huawei joined the CSA in 2012 and was upgraded to an executive corporate member in January 2017. And, HUAWEI CLOUD has passed the Cloud Security Alliance CSA STAR Gold Certification (CSA - Cloud Security Alliance, STAR - Security, Trust & Assurance Registry), which adds the Cloud Security Control Matrix (CCM - Cloud Control Matrix) and other security requirements to

		duration to retain log data, events that would trigger these systems to send alerts, monitoring intervals/ frequency, and how identified cyber-incidents I breaches will be contained, treated, documented, and reported. g. Determine a baseline of operations and expected data flows for users, systems, and network of the identified systems. This includes but not limited to logon hours, network traffic threshold, level of processor utilization, etc. h. Implement across all-delivery channels a risk-based transaction monitoring mechanism which shall securely notify customers of all payment or fund transfer transactions above a specified value defined by customers. i. Establish a non-intrusive real-time monitoring mechanism to collect, correlate, and detect anomalous user, administrator, system, and process/service activities on system, database, and network in a timely manner while verifying the effectiveness of protective measures in place. j. Ensure that the mechanism provides Value Added Services (VAS) such as separating real events from nonimpact events (false positive), locating and containing events, sending alerts to appropriate staff for investigation, remediation, reporting, keeping historical data for the purpose of forensics,	ISO/IEC The certification adds the Cloud Security Control Matrix (CCM - Cloud Control Matrix) and other security requirements to ISO/IEC 27001, covering 16 control areas including risk governance, data security, application security, infrastructure security, development and design. Achieving CSA STAR Gold certification signifies that Huawei Cloud's operational security management and technical capabilities have been recognized by international authorities, and

		and managing operational risks. k. Monitor the physical environment of assets-server room, network devices, data center, disaster recovery site, and off-site storage location -to detect potential threats in a timely manner. 1. Establish an effective and efficient non-intrusive mechanism to detect and perform remediation actions on malicious codes and unauthorized mobile codes on all systems (including those on the DMZ). For signature-based solutions, frequency of update shall be at least daily. m. DMBs and PSPs that intends to or have cloud service providers shall be guided by the continuous security monitoring recommendation of Cloud Security Alliance (CSA).	its security compliance is at a world-leading level.

DBM and PSP Guidelines Appendix IV 1	Enhancing Cybersecurity Resilience	8. Incident Response: This is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an „incident") with an objective of reducing damage, recovery time and incident costs. For an effective and efficient Incident Response (IR), a DMB/PSP shall: a. Review its Disaster Recovery and Business Continuity plan documents (DR/BCP) with the business (stakeholders) to ensure they are adequate and effective to support cybersecurity resilience. b. Create a DR/BCP test calendar to ascertain the effectiveness and efficiency of the Disaster Recovery and Business Continuity plans. c. Test the DR/BCP. Lessons learned shall be incorporated into the DR/BCP documents as an improvement. d. Develop an IR policy with stakeholders. The IR policy shall stipulate: i. the creation of a cyber-incident response plan; approved by the Board of Directors; ii. Senior management and business process owners definition of an Acceptable Interruption Window (AIW) for all categories of cyber-incidents and performance metric at each stage of the IR process; ach stage of the IR process; iii. the establishment of a dedicated team whose focus shall be on detecting and	FIs shall develop and review disaster recovery and business continuity plan documents and employ automated detection tools for early detection of cyber incidents. HUAWEI CLOUD has a professional security incident response team available 7*24 and a corresponding pool of security expert resources for response. 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 but not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, HUAWEI CLOUD will provide the incident report to the customer according to the specific situation. In addition to the high availability infrastructure, data redundancy and backup, and DR among AZs, Huawei Cloud also has a formal business continuity plan (BCP) and conducts BCP drills periodically. This plan, which applies to major disasters such as earthquakes or public health crises, ensures continued operations of HUAWEI CLOUD services and

		responding to cyber-incident; iv. adequate and continuous training of the IR team on how to respond, report cyber-incidents, and conduct trend analysis to thwart future occurrence; v. conducting cybersecurity drills based on the approved cyber-incident response plan and test schedule to ascertain its viability, effectiveness and efficiency; vi. the adoption of automated detection tool such as network and system (endpoint) scanners; and alerts from Log Management solutions, Firewall, Intrusion Detection/Intrusion Prevention systems (ID/IPS), etc. for effective early detection of cyber-incidents; vii. appropriate chain of custody when collecting, analyzing and reporting cyber incident in a manner that is legally admissible; and viii. how crisis information shall be communicated and shared with stakeholders including the CBN and the public.	safeguards customers' service and data security. HUAWEI CLOUD has a DR plan (DRP) as well, and conducts DRP tests periodically. For example, first bring the cloud platform infrastructure and cloud services offline in a certain geographic location or region to simulate a disaster, then, perform system operations and migration as specified in the DRP, and lastly, verify the service and business operations functions in the presumably disaster-impacted region. Test results are then annotated and archived for continuous improvement of the DRP.

Draft OFI Guidelines Appendix III 8	Enhancing Cybersecurity Resilience	8. Incident Response (IR): This is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an „incident") with an objective of reducing damage, recovery time and incident costs. For an effective and efficient incident response, an OFI shall: a. Review its Disaster Recovery and Business Continuity plan documents (DR/BCP) with the business (stakeholders) to ensure they are adequate and effective to support cybersecurity resilience. b. Create a DR/BCP test calendar to ascertain the effectiveness and efficiency of the Disaster Recovery and Business Continuity plans. c. Test the DR/BCP. Lessons learned shall be incorporated into the DR/BCP documents as an improvement. d. Develop an IR policy with stakeholders. The IR policy shall stipulate: i. the creation of a cyber-incident response plan; approved by the Board of Directors; ii. Senior management and business process owners definition of an Acceptable Interruption Window (AIW) for all categories of cyber-incidents; and performance metric at each stage of the IR process; iii. the establishment of a dedicated team whose focus shall be on detecting and	

		responding to cyber-incident; iv. adequate and continuous training of the IR team on how to respond, report cyber¬ incidents, and conduct trend analysis to thwart future occurrence; v. conducting cybersecurity drills based on the approved cyber-incident response plan and test schedule to ascertain its viability, effectiveness and efficiency; vi. the adoption of automated detection tool such as network and system (endpoint) scanners; and alerts from Log Management solutions, Firewall, Intrusion Detection/Intrusion Prevention systems (ID/IPS) etc. for effective early detection of cyber-incidents; vii. appropriate chain of custody when collecting, analyzing and reporting cyber incident in a manner that is legally admissible; and viii. how crisis information shall be communicated and shared with stakeholders including the CBN and the public.	

6.3 Cyber-Threat Intelligence

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response

DBM and PSP Guidelines 4	Cyber-Threat Intelligence	A DMB/PSP is required to possess an objective knowledge – based on fact – of all emerging threats, cyber-attacks, attack vector, mechanisms and indicators of attack/compromise to its information assets which shall be used to make informed decisions. To this end, DMBs and PSPs are required to: 4.3.1. Establish a Cyber-Threat Intelligence (CTI) programme which shall proactively identify, detect and mitigate potential cyber-threats and risks. 4.3.2. Establish a CTI policy (as part of the cybersecurity policy) approved by the Board of Directors to aid proactive identification of emerging cyber threat, trends, patterns, risks, and possible impact. 4.3.3. Identify and document various CTI Sources. See Appendix VI for details. 4.3.4. Take informed decisions based on the CTI programme as it provides valuable information on areas susceptible to cyber-attacks, latest threats, attack vector, etc. Decisions may include: reviewing the Bring Your Own Device (BYOD) policy; conducting emergency awareness training, vulnerability assessment, and penetration testing; review of vendor source codes, cyber-incident response plan, BCP/DR plans, vendor SLA; and increased system logging, etc. 4.3.5. Promptly report all impending and challenging cyber-threats to their	FIs shall establish threat intelligence programs to proactively identify, detect and mitigate potential cyber threats and risks, and report them to regulators. HUAWEI CLOUD provides **Managed Threat Detection(MTD)**, by accessing the IAM logs, DNS logs, CTS logs, OBS logs, and VPC logs generated by users' operations in Huawei Cloud in the target area, the IP or domain name of visitors in the logs will be continuously detected for potential malicious activities and unauthorized behaviors, and any detected abnormality will be alerted in time. It integrates log detection models, such as AI detection engine, threat intelligence, and detection policy, to identify threats to Intelligent detection from multiple cloud services (Includes IAM service, DNS service, CTS service, OBS service, VPC service) The abnormal access behaviors implied in the log data, proactively discover potential threats, generate alert information for access behaviors that may have threats, and output alert results. Users can verify and process the alarm information through the alarm descriptions, so that potential threats can be handled and service security can be upgraded and reinforced in a timely manner before causing major losses such as information leakage, thus protecting users' account security and ensuring stable service operation.

		information assets to the Director of Banking Supervision of Central Bank of Nigeria using the Cyber-threat Intelligence Reporting template in Appendix VII after its endorsement by appropriate authorities.	

Draft OFI Guidelines 6	Cyber-Threat Intelligence	An OFI is required to possess an objective knowledge-based on fact-of all emerging threats, cyber-attacks, attack vector, mechanisms and indicators of attack/compromise to its information assets which shall be used to make informed decisions. To this end, OFIs are required to: 6.1 Establish a Cyber-Threat Intelligence (CTI) programme which shall proactively identify, detect and mitigate potential cyber-threats and risks. 6.2 Establish a CTI policy (as part of the cybersecurity policy) approved by the Board of Directors to aid proactive identification of emerging cyber threats, trends, patterns, risks and possible impact. 6.3 Identify and document various CTI Sources. See Appendix V for details. 6.4 Take informed decisions based on the CTI programme as it provides valuable information on areas susceptible to cyber-attacks, latest threats, attack vector, etc. Decisions may include: conducting emergency awareness training, vulnerability assessment, and penetration testing; review of vendor source codes, cyber-incident response plan. Business Continuity/Disaster Recovery Plans (BCP/DRP), vendor Service Level Agreement (SLA); and increased system logging, reviewing the Bring Your Own Device (BYOD) policy, etc.	

		6.5 Promptly report all potential cyber-threats to their information assets to the Director, Other Financial Institutions Supervision Department of the Central Bank of Nigeria using the Cyber¬ threat Intelligence Reporting template in Appendix I.	

DBM and PSP Guidelines Appendix VI Draft OFI Guidelines Appendix V	Cyber-Threat Intelligent Sources	Internal Threat Intelligence (TI) sources 1. The SOC shall not just house sophisticated tools but equipped with a Security Information and Event Management (SIEM) solution that aggregates data from various security feeds to provide real-time analysis of security alert. Where applicable, the SOC shall be able to perform prompt remediation service. 2. For intuitive correlations and prompt visibility of the bank" security posture, feeds to the SIEM shall also include logs from network devices, vulnerability assessment systems; application and database scanners; penetration testing tools; IDS/IPS; and enterprise antivirus system. 10. The SOC shall have well documented processes to triage various types of cyber-incidents with appropriate response approved by the business process owners for operational consistency; identify, analyze and report emerging threats gather and preserve evidence for Forensic Investigation 11. There shall be a capacity planning tool/ process that communicates SOC infrastructure (SIEM) storage to enable the SOC team balance task	FIs threat intelligence sources should include both internal and external; a security operations center (SOC) should be established, containing tools, security information and incident management solutions. HUAWEI CLOUD provides **Managed Threat Detection(MTD)**, by accessing the IAM logs, DNS logs, CTS logs, OBS logs, and VPC logs generated by users' operations in Huawei Cloud in the target area, the IP or domain name of visitors in the logs will be continuously detected for potential malicious activities and unauthorized behaviors, and any detected abnormality will be alerted in time. It integrates log detection models, such as AI detection engine, threat intelligence, and detection policy, to identify threats to Intelligent detection from multiple cloud services (Includes IAM service, DNS service, CTS service, OBS service, VPC service) .The abnormal access behaviors implied in the log data, proactively discover potential threats, generate alert information for access behaviors that may have threats, and output alert results. Users can verify and process the alarm information through the alarm descriptions, so that potential threats can be handled and service security can be upgraded and reinforced in a timely manner before causing major losses such as information leakage, thus protecting users' account security and ensuring stable service operation.

		workload with available resources. External TI sources: 1. A DMB/PSP/OFI shall subscribe to external T1 providers such as data feeds from IT vendors; intelligence sharing group such as the ngCERT, FS-ISAC. ICS-CERT; other MBs/PSPs/ OFIs; and relevant agencies to keep them informed of emerging cyber-threats and vulnerabilities. 2. Caution shall be exercised on open-source cyber-threat intelligence feeds due to high rate of false positive and or false negative alerts.	HUAWEI CLOUD provides **Cloud Eye (CES)** to provide users with a three-dimensional monitoring platform for elastic cloud servers, bandwidth, and other resources to help users capacity calendar. CES provides real-time monitoring alerts, notifications, and personalized report views to accurately grasp the status of business resources.

6.4 Metrics, Monitoring & Reporting

No.	Control Domain	Specific Control Requirements	HUAWEI CLOUD Response
DBM and PSP Guidelines 5.4	Metrics, Monitoring & Reporting	5.4. A reporting process that defines reporting and communication channels shall be established for the dissemination of security-related material such as changes in policies, standards, procedures, new or emerging threats and vulnerabilities.	FIs should define reporting processes for reporting and communication channels to disseminate security-related material. HUAWEI CLOUD, as a cloud service provider, has developed an incident reporting process, HUAWEI CLOUD has a professional security incident response team available 7*24 and a corresponding pool of security expert resources for response. HUAWEI CLOUD formulates the classification and escalation principles of information security incidents,

Draft OFI Guidelines 7.4	Metrics, Monitoring & Reporting	7.4 A reporting process that defines reporting and communication channels shall be established for the dissemination of security-related material such as changes in policies, standards, procedures, new or emerging threats and vulnerabilities.	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 but not limited to a description of the event, the cause, impact, measures taken by HUAWEI CLOUD and the measures recommended for customers. After the incident is resolved, HUAWEI CLOUD will provide the incident report to the customer according to the specific situation.

7 Conclusion

This white paper describes how HUAWEI CLOUD provides cloud services that meet regulatory requirements of the financial industry in Nigeria and shows that HUAWEI CLOUD complies with key regulatory requirements issued by the Central Bank of Nigeria (CBN). This white paper aims to help customers learn more about HUAWEI CLOUD's compliance status with Nigeria'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 white paper also guides customers on how to design, build and deploy a secure cloud environment that meets the regulatory requirements of CBN on HUAWEI CLOUD, and assists customer to better identify security responsibilities together with HUAWEI CLOUD.

This white paper is for reference only and does not have any legal effect or constitute any legal advice. Customers should assess their own situation when using cloud services and be responsible for ensuring compliance with relevant financial industry regulatory requirements when using HUAWEI CLOUD.

8 Version History

Date	Version	Description
August 2022	1.0	First release

