

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

Issue	1.0
Date	2023-02-09



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property 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

1.1 Background and Purpose of Publication..... 1

1.2 Introduction of Applicable Kenya Financial Regulatory Requirements..... 1

1.3 Definition..... 2

2 HUAWEI CLOUD Security and Privacy Compliance..... 3

3 HUAWEI CLOUD Security Responsibility Sharing Model..... 37

4 HUAWEI CLOUD Global Infrastructure..... 39

5 How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of Risk Management Guidelines..... 40

5.1 Policies and procedures..... 41

5.2 Measurement, monitoring and control..... 43

5.3 Risk assessment, measurement and monitoring..... 45

6 How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of IRA Risk Management and Internal Control Guidelines..... 57

6.1 Risk management system..... 58

6.2 Risk Mitigation and Control..... 60

7 How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of CBK Prudent Outsourcing Guidelines CBK PG 16..... 63

8 How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of GUIDANCE NOTE ON CYBERSECURITY..... 74

9 How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of Internet Security Guide for Payment Service Providers..... 79

10 Conclusion..... 87

11 Version History..... 88

1 Overview

1.1 Background and Purpose of Publication

With the development of technology, the use of cloud computing technology and services has become the norm for financial institutions in Kenya. While cloud computing has brought great convenience to the development of financial institutions, network security incidents have also emerged. In order to standardize the application of information technology in the financial industry, the Central Bank of Kenya (CBK) and the Insurance Regulatory Authority (IRA) have issued a series of regulatory regulations on network security, information technology risk management and other aspects of financial institutions in Kenya.

As a cloud service provider, HUAWEI CLOUD is committed to helping financial customers meet these regulatory requirements and continues to provide financial customers with cloud services and business operation environments that comply with financial industry standards. This article will describe in detail how HUAWEI CLOUD will help Kenyan financial institutions to meet regulatory requirements when using cloud services.

1.2 Introduction of Applicable Kenya Financial Regulatory Requirements

The Central Bank of Kenya (CBK) oversees banks, credit institutions and payment operators; The Insurance Regulatory Authority (IRA) manages and supervises the insurance industry. The Central Bank of Kenya and the Insurance Regulatory Authority have issued regulations that impose requirements on financial institutions.

- **RISK MANAGEMENT GUIDELINES** In January 2013, the Central Bank of Kenya provided all institutions with guidelines on the minimum requirements for risk management systems and frameworks. This guideline covers risk management framework, strategic risk management, credit risk management, liquidity risk management, market risk management, operational risk management, information and communication technology risk, compliance risk, etc.

- **IRA Guidelines on Risk Management and Internal Controls IRA/PG/11** In June 2013, the Insurance Regulatory Bureau required insurance companies to have effective risk management and internal control systems as part of the overall corporate management framework, including effective risk management, compliance, and internal audit.
- **CBK Prudential Guidelines on Outsourcing CBK/PG/16 (Outsourcing Guidelines) which is applicable to banks.** The fourth part of the specific requirements restricts the internal control and prudential standards, risk management practices of outsourcing financial services, regulatory and supervisory requirements, offshore outsourcing of financial services and other related security requirements.
- **GUIDANCE NOTE ON CYBERSECURITY** In August 2017, the Central Bank of Kenya clarified the minimum requirements that institutions should follow when formulating and implementing strategies, policies, procedures and related activities aimed at mitigating network risks, mainly covering risk management, outsourcing, information and communication technology, internal control, corporate governance and other fields.
- **CBK Guidelines on Cybersecurity for Payment Service Providers (PSP Guidelines)** In November 2019, the Central Bank of Kenya set the minimum standards that payment service providers (PSPs) should adopt to develop an effective network security governance and risk management framework.

1.3 Definition

- **HUAWEI CLOUD**
HUAWEI CLOUD is the cloud service brand of the HUAWEI marquee, committed to providing stable, secure, reliable, and sustainable cloud services.
- **Customer**
Refers to registered users who have entered into commercial relations with HUAWEI CLOUD
- **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).
- **Service provider**
It refers to the use of a third party (an associated entity within the company group or an entity outside the company group) to continue to carry out activities that are now or will normally be undertaken by the institution itself.
- **Business continuity**
It refers to the continuous and uninterrupted operation of the enterprise.
- **Business continuity management**
A comprehensive business approach, including policies, standards, frameworks and procedures, to ensure that specific operations can be maintained or resumed in a timely manner in the event of disruption. Its purpose is to minimize the business, financial, legal, reputation and other substantive consequences arising from the interruption.

2 HUAWEI CLOUD Security and Privacy Compliance

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

HUAWEI CLOUD services and platforms have obtained the following certifications:

Global standard certification

Certification	Description
ISO 20000-1:2011	ISO 20000 is an international recognized information technology Service Management System (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS to make sure cloud service providers(CSPs) can provide effective IT services to meet the requirements of customers and businesses.
ISO 27001:2013	ISO 27001 is a widely used international standard that specifies requirements for information security management systems. This standard provides a method of periodic risk evaluation for assessing systems that manage company and customer information.
ISO 27017:2015	ISO 27017 is an international certification for cloud computing information security. The adoption of ISO 27017 indicates that HUAWEI CLOUD has achieved internationally recognized best practices in information security management.

Certification	Description

I
S
O
2
2
3
0
1
i
2
0
1
2
n
t
e
r
n
a
t
i
o
n
a
l
l
y
r
e
c
o
g
n
i
z
e
d
b
u
s
i
n
e
s
s
c
o
n
t
i

Certification	Description

n
u
i
t
y
m
a
n
a
g
e
m
e
n
t
s
y
s
t
e
m
s
t
a
n
d
a
r
d
t
h
a
t
h
e
l
p
s
o
r
g
a
n
i
z
a
t
i
o
n

Certification	Description

s
a
v
o
i
d
p
o
t
e
n
t
i
a
l
i
n
c
i
d
e
n
t
s
b
y
i
d
e
n
t
i
f
y
i
n
g
,
a
n
a
l
y
z
i
n
g
,
a
n

Certification	Description

d
a
l
e
r
t
i
n
g
r
i
s
k
s
,
a
n
d
d
e
v
e
l
o
p
s
a
c
c
o
m
p
r
e
h
e
n
s
i
v
e
B
u
s
i
n
e
s
s
C
o

Certification	Description

n
t
i
n
u
i
t
y
p
l
a
n
(
B
C
P
)
t
o
e
f
f
e
c
t
i
v
e
l
y
r
e
s
p
o
n
d
t
o
d
i
s
r
u
p
t
i
o
n
s

Certification	Description

o
t
h
a
t
e
n
t
i
t
i
e
s
c
a
n
r
e
c
o
v
e
r
r
a
p
i
d
l
y
;
k
e
e
p
c
o
r
r
e
b
u
s
i
n
e
s
s
r
u
n

Certification	Description

n
i
n
g
,
a
n
d
m
i
n
i
m
i
z
e
l
o
s
s
a
n
d
r
e
c
o
v
e
r
y
c
o
s
t
s
.

Certification	Description
SOC audit	The SOC audit report is prepared by a third-party auditor according to the American Institute of Certified Public Accountants(AICPA), an independent audit report on the system and internal control of outsourcing service providers. HUAWEI CLOUD has obtained three authoritative certifications of SOC 1 Type II, SOC 2 Type II and SOC 3 authentication audit reports. Among them, the five control attributes of SOC 2 have all passed the audit, which is the first in the world. This shows that the information security management capability of HUAWEI CLOUD platform has reached the highest internationally recognized standard and can provide you with world-class security and privacy protection and services.
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.

Table 1-1: SOC audit and PCI DSS Certification

Certification	Description
International Common Criteria EAL 3+ Certification	Common Criteria certification is a highly recognized international standard for information technology products and system security. HUAWEI CLOUD Fusion Sphere passed Common Criteria EAL 3+ certification, indicating that the HUAWEI CLOUD software platform is highly recognized worldwide.

British Standards Institution (BSI), an authoritative

Certification	Description

a
n
d
a
r
d
d
e
v
e
l
o
p
m
e
n
t
a
n
d
p
r
e
p
a
r
a
t
i
o
n
b
o
d
y
a
s
w
e
l
l
a
s
a
w
o
r
l
d
w

Certification	Description

i
d
e
c
e
r
t
i
f
i
c
a
t
i
o
n
s
e
r
v
i
c
e
p
r
o
v
i
d
e
r
,
d
e
v
e
l
o
p
e
d
C
S
A
S
T
A
R
c
e
r

Certification	Description

t
i
f
i
c
a
t
i
o
n
.
T
h
i
s
c
e
r
t
i
f
i
c
a
t
i
o
n
a
i
m
s
t
o
i
n
c
r
e
a
s
e
t
r
u
s
t
a
n
d
t
r

Certification	Description

a
n
s
p
a
r
e
n
c
y
i
n
t
h
e
c
l
o
u
d
c
o
m
p
u
t
i
n
g
i
n
d
u
s
t
r
y
a
n
d
e
n
a
b
l
e
s
c
l
o

Certification	Description

u
d
c
o
m
p
u
t
i
n
g
s
e
r
v
i
c
e
p
r
o
v
i
d
e
r
s
t
o
d
e
m
o
n
s
t
r
a
t
e
t
h
e
i
r
s
e
r
v
i

Certification	Description
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.

c
e
m
a
t
u
r
i
t
y
.

Certification	Description

I
S
O
2
9
1
5
1
i
2
6
7
n
t
e
r
n
a
t
i
o
n
a
l
p
r
a
c
t
i
c
a
l
g
u
i
d
e
t
o
t
h
e
p
r
o
t
e
c

Certification	Description

t
i
o
n
o
f
p
e
r
s
o
n
a
l
i
d
e
n
t
i
t
y
i
n
f
o
r
m
a
t
i
o
n
.T
h
e
a
d
o
p
t
i
o
n
o
f
I
S
O

Certification	Description

2
9
1
5
1
c
o
n
f
i
r
m
s
H
U
A
W
E
I
C
L
O
U
D
's
i
m
p
l
e
m
e
n
t
a
t
i
o
n
o
f
i
n
t
e
r
n
a
t
i
o

Certification	Description

n
a
l
l
y
r
e
c
o
g
n
i
z
e
d
m
a
n
a
g
e
m
e
n
t
m
e
a
s
u
r
e
s
f
o
r
t
h
e
e
n
t
i
r
e
l
i
f
e
c

Certification	Description
ISO 27701:2019	ISO 27701 specifics requirements for the establishment, implementation, maintenance and continuous improvement of a privacy-specific management system. The adoption of ISO 27701 demonstrates that HUAWEI CLOUD operates a sound system for personal data protection.
BS 10012:2017	BS10012 is the personal information data management system standard issued by BSI. The BS10012 certification indicates that HUAWEI CLOUD offers a complete personal data protection system to ensure personal data security.
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.

y
c
l
e
o
f
p
e
r
s
o
n
a
l
d
a
t
a
p
r
o
c
e
s
s
i
n
g
.

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 for the Capability of Protecting Cloud Service User Data (TRUCS) (China)	This certification evaluates a CSP's ability to protect cloud data. Evaluation covers pre-event prevention, in-event protection, and post-event tracking.

Certification	Description

I
T
S
C
l
o
u
d
C
o
m
p
u
t
i
n
g
S
e
r
v
i
c
e
C
a
p
a
b
i
l
i
t
y
E
v
a
l
u
a
t
i
o
n
b
y
H
e

Certification	Description

Certification	Description

h
è
m
a
h
t
s
f
o
r
l
n
f
o
r
m
a
t
i
o
n
T
e
c
h
n
o
l
o
g
y
C
l
o
u
d
C
o
m
p
u
t
i
n
g
C
l
o
u
d

Certification	Description

S
e
r
v
i
c
e
O
p
e
r
a
t
i
o
n
a
n
d
o
t
h
e
r
r
e
l
e
v
a
n
t
n
a
t
i
o
n
a
l
s
t
a
n
d
a
r
d
s
.

Certification	Description
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.

O
S
P
A
R
C
e
a
n
a
f
i
d
a
t
i
r
e
p
o
s
t
i
n
g
a
p
e
d
b
y
t
h
e
A
s
s
o
c
i
a
t
i
o
n
o
f

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.

B
a
n
k
s
i
n
S
i
n
g
a
p
o
r
e
(
A
B
S
)
t
o
o
u
t
s
o
u
r
c
i
n
g
s
e
r
v
i
c
e
p
r
o
v
i
d
e
r
s

Certification	Description

HUAWEI CLOUD passed the guidelines (ABS Guidelines) of the

Certification	Description

e
A
s
s
o
c
i
a
t
i
o
n
o
f
B
a
n
k
s
o
f
S
i
n
g
a
p
o
r
e
(
A
B
S
)
o
n
c
o
n
t
r
o
l
l
i
n
g
t
h

Certification	Description

e
o
b
j
e
c
t
i
v
e
s
a
n
d
p
r
o
c
e
s
s
e
s
o
f
o
u
t
s
o
u
r
c
i
n
g
s
e
r
v
i
c
e
p
r
o
v
i
d
e

Certification	Description

r
s
,
p
r
o
v
i
n
g
t
h
a
t
H
U
A
W
E
I
C
L
O
U
D
i
s
a
n
o
u
t
s
o
u
r
c
i
n
g
s
e
r
v
i
c
e
p
r
o

Certification	Description

vidert hat compliance with the control measures Certifications

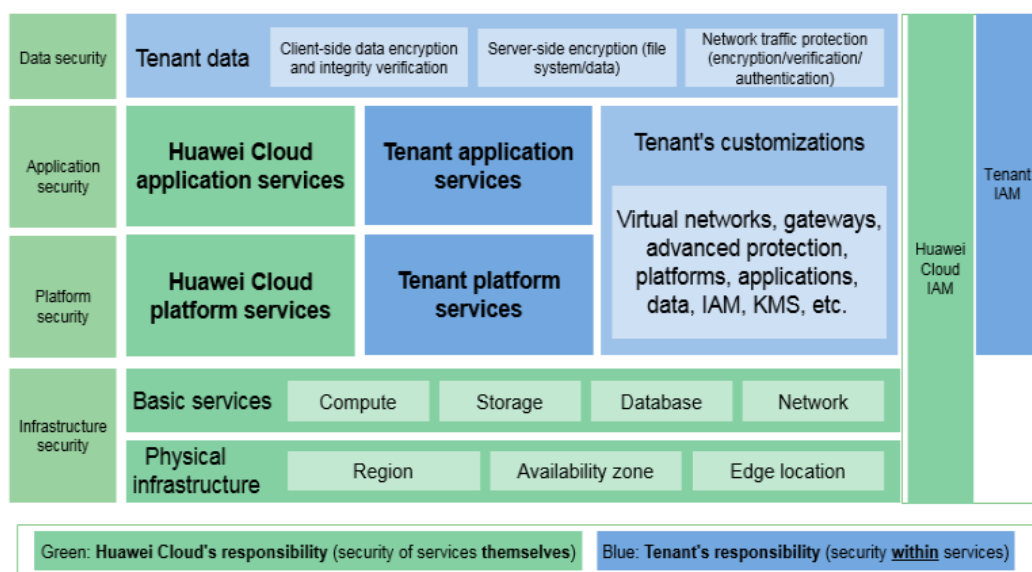
Certification	Description

n
t
h
e
A
B
S
G
u
i
d
e
l
i
n
e
s
.

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

3 HUAWEI CLOUD Security Responsibility Sharing Model

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



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

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

and data layers, in addition to the identity and access management (IAM) cross layer function.

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

For details on the security responsibilities of both Customers and HUAWEI CLOUD, please refer to the [HUAWEI CLOUD Security White Paper](#) released by HUAWEI CLOUD.

4 HUAWEI CLOUD Global Infrastructure

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

5

How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of Risk Management Guidelines

The Central Bank of Kenya issued the Risk Management Guidelines in January 2013, which provide all institutions with guidelines on the minimum requirements for risk management systems and frameworks. This guideline covers risk management framework, strategic risk management, credit risk management, liquidity risk management, market risk management, operational risk management, information and communication technology risk, compliance risk, etc.

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

5.1 Policies and procedures

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
6.3.1 Policy on outsourcing	The Board of Directors and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are developed to manage the risks of outsourcing activities.	<p>The client's senior management should establish outsourcing risk management policies, including:</p> <ul style="list-style-type: none"> (a) Judge whether the activities can be outsourced and carry out outsourcing activities as required; (b) Conduct due diligence when selecting service providers. (c) To ensure the ownership and confidentiality of data, as well as the right to terminate. (d) Programmes to manage and monitor risks associated with outsourcing arrangements, including the financial situation of service providers. (e) There is a stable and secure environment with service providers. (f) Formulate feasible emergency plan; And (g) Implement comprehensive contracts and/or service level agreements to clarify the allocation of responsibilities between service providers and banks. 	<p>HUAWEI CLOUD will arrange special personnel to actively cooperate with financial institutions in their due diligence. In order to enable users to enjoy a secure and reliable cloud platform and cloud services, HUAWEI CLOUD has built a complete security system from security technologies, security systems, personnel management and other aspects in accordance with authoritative security standards around the world, and has obtained numerous security certifications at home and abroad. Huawei advocates the concept and practice of "everyone understands security" within the company, creating a security culture that is everywhere, dynamic and competitive. It also runs through HUAWEI CLOUD recruitment and selection, employee</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			<p>induction, induction training, continuous training, internal transfer and resignation.</p> <p>HUAWEI CLOUD provides an online version of the HUAWEI CLOUD Service Level Agreement, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. The audit and supervision rights and interests of customers and their regulators on HUAWEI CLOUD will be agreed in the agreement signed with customers according to the actual situation. HUAWEI CLOUD has obtained ISO27001, ISO27017, ISO27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by a third party every year.</p>

5.2 Measurement, monitoring and control

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
6.4.3 Control and mitigation	An organization should develop a detailed business continuity plan. Recovery plans and business recovery priorities must be determined, and emergency procedures must be tested and practiced to minimize business and operational disruption caused by serious operational risk events. The recovery plan and event response procedures shall be evaluated regularly and updated when business operations, systems and networks change.	The customer shall have a business continuity plan, and must determine the priority of business recovery and conduct emergency drills. The recovery plan and event response procedures shall be evaluated regularly and updated when business operations, systems and networks change.	As a cloud service provider, HUAWEI CLOUD provides financial institution customers with cloud services on which their business depends. Therefore, except for outsourcing interruption or accidental termination caused by irresistible factors, HUAWEI CLOUD has developed a business continuity management system that conforms to its own business characteristics to provide customers with continuous and effective services and ensure the development of customer business. HUAWEI CLOUD will conduct business continuity publicity and training in the organization every year, as well as regular emergency drills and tests, to continuously optimize the emergency response mechanism.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
6.4.4 Pressure Test	Institutions should regularly undertake stress testing for a variety of short- and long-term institution-specific operational risk stress scenarios to identify potential sources of operational risk and to ensure that institutions are prepared to continue operations following minor and significant operational risk events. Institutions should use the results of the stress tests to adjust their operational risk management strategies, policies, and positions and to develop effective contingency plans.	The customer should conduct regular stress tests to identify and locate vulnerable parts of the business, improve understanding of the risk situation, monitor changes in risk, and adjust contingency plans in a timely manner.	As a cloud service provider, HUAWEI CLOUD provides financial institutions with cloud services on which their services depend. Except for outsourcing interruption or unexpected termination caused by force majeure, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics to continuously and effectively provide services for customers. Ensure the development of customer business. HUAWEI CLOUD conducts business continuity publicity and training in the organization every year, and regularly conducts emergency drills and tests to continuously optimize the emergency response mechanism.

5.3 Risk assessment, measurement and monitoring

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
7.4.2 Risk measurement	<p>The institution should establish a continuous risk measurement and monitoring mechanism. The mechanism should include:</p> <p>Pre-implementation and post-implementation review of ICT projects; Benchmarking of system performance on a regular basis; Reports of incidents and complaints related to ICT services; Reports of internal audit, external audit, and reports of problems found by CBK; Arrangements with suppliers and business units; Periodically review Service Level Agreements (SLAs).</p> <p>The possible impact of new technological developments and new threats on software development.</p> <p>Review operational risks and management controls in a timely manner in the business area.</p> <p>Regularly assess the risk profile of IT outsourcing projects.</p>	<p>The Client shall establish risk management and risk monitoring mechanisms to review the implementation of ICT projects, system performance, reports of incidents and complaints related to ICT services, reports of internal/ external audits, and issues identified by CBK, arrangements with suppliers and business units, service level agreements (SLAs).</p> <p>Regularly assess the risk profile of IT outsourcing projects.</p>	<p>HUAWEI CLOUD develops and maintains an internal risk management framework to identify, analyze, and manage identified risks. HUAWEI CLOUD conducts a formal risk assessment at least once a year and develops a risk calculation and classification process to determine the possibility and impact of identified risks. The likelihood and impact associated with each risk is determined independently and each risk category should be considered. Risk criteria to reduce risk to an acceptable level, including resolution times, should be developed, documented and approved</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			by management. In addition, HUAWEI CLOUD organizes meetings at least once a month to discuss cyber security and privacy protection risk assessment. HUAWEI CLOUD takes and records follow-up actions to ensure that risks are properly managed in accordance with Huawei's risk management requirements.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
7.8 Audit Trail	<p>The institution should establish a set of policies and procedures to control activity records in all production systems to support effective auditing, security forensic analysis, and fraud prevention. Logging can be implemented on different levels of software and on different computers and network devices, which are divided into two broad categories.</p> <p>1) Transaction logs are generated by program software and database management systems and contain authentication attempts, modifications to data and error information. The transaction log shall be maintained in accordance with the information retention policy established by the law of that country.</p> <p>2) System logs are generated by operating systems, database management systems, firewalls, intrusion detection systems, and routers, including authentication attempts, system events, network events, and error information.</p>	<p>Customers can use HUAWEI CLOUD Identity and Access Management to manage privileged accounts in a more effective manner. You can also use Cloud Trace Service(CTS) to record operations on cloud service resources for query, audit, and backtrack operations.</p>	<p>To meet customers' compliance requirements, administrators of HUAWEI CLOUD-related systems must pass two-factor authentication when logging in to the system before accessing the management plane through the locked-down server. All operations are recorded in logs and sent to the centralized log audit system in a timely manner. The audit system has powerful data storage and query capabilities, ensuring that all logs are stored for more than 180 days and can be queried in real time within 90 days. In addition, HUAWEI CLOUD has a dedicated internal audit department that regularly audits all activities in the O&M process.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
7.9 Encryption Technology	<p>Organizations should have the ability to use encryption technology to reduce the risk of loss of confidential information in information and communications systems or during their transmission. Appropriate encryption facility management procedures shall be established to ensure that encryption facilities in use meet international security standards or requirements.</p> <p>The staff responsible for the management of encrypted facilities are well trained and vetted. This is verified by professional and academic certificates, proof of conduct by independent recommenders, and proof of good behavior.</p> <p>Encryption is strong enough to protect the confidentiality of information. Effective and efficient key management procedures, especially key life cycle management and certificate life cycle management.</p>	<p>To meet customers' requirements for data confidentiality, HUAWEI CLOUD provides server-side encryption and integrates the key management function of Data Encryption Workshop (DEW). DEW centrally manages keys throughout the lifecycle. DEW is a comprehensive cloud data encryption service. It provides functions such as dedicated encryption, key management, and key pair management. Its keys are protected by hardware security modules (HSMs) and are integrated with many HUAWEI CLOUD services. Users can also use this service to develop their own encryption applications.</p>	<p>HUAWEI CLOUD complies with security laws and regulations of the local country or region and industry regulatory requirements, and establishes and manages a complete, highly reliable, and sustainable data security assurance system in terms of organization, process, specifications, technology, compliance, and ecosystem by referring to industry best practices. HUAWEI CLOUD adopts a series of protection mechanisms to ensure the storage security of tenant data.</p> <p>HUAWEI CLOUD has established encryption policies and key management mechanisms for protecting data on technical devices, and specified encryption</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
		Without authorization, no one except the customer can obtain the key to decrypt data, which ensures data security on the customer cloud.	<p>levels and encryption methods. If data is transmitted from the client to the server and between the server on the Huawei cloud platform through the common information channel, the following methods are used to protect data during transmission:</p> <p>1. Virtual Private Network (VPN): A secure and encrypted communication tunnel that complies with industry standards is established between a remote network and a VPC, seamlessly extending the existing data center to HUAWEI CLOUD. Currently, HUAWEI CLOUD uses hardware-based IKE and IPSec VPN to encrypt data</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			<p>transmission channels.</p> <p>2. Application layer TLS and certificate management: HUAWEI CLOUD provides REST and Highway data transmission. The preceding data transmission modes support encrypted transmission using Transport Layer Security (TLS) 1.2 and X.509 certificate-based identity authentication for target websites. In addition, HUAWEI CLOUD O&M personnel use HTTPS to prevent data leakage during transmission when connecting to the customer's VPC environment.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
7.15 Business Continuity Management	Agencies should make appropriate arrangements, depending on the nature, scale and complexity of their operations, to ensure that they can continue to operate and meet their regulatory obligations in the event of an unexpected disruption in information and communications technology. These arrangements should be updated and tested regularly to ensure their effectiveness.	The customer should develop a business continuity management plan and regularly update it to ensure the effectiveness of business continuity management.	As a cloud service provider, HUAWEI CLOUD provides financial institutions with cloud services on which their services depend. Except for outsourcing interruption or unexpected termination caused by force majeure, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics to continuously and effectively provide services for customers. Ensure the development of customer business. HUAWEI CLOUD conducts business continuity publicity and training in the organization every year, and regularly conducts emergency

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			drills and tests to continuously optimize the emergency response mechanism.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
7.16 Outsourcing	<p>1) Risk analysis</p> <p>Prior to entering into a material change to the outsourcing agreement, the institution shall:</p> <p>Analysis of how the arrangement would fit into its information and communications technology organization and reporting structure; business strategy; Overall risk profile; and the ability to meet their regulatory obligations.</p> <p>Consider whether these arrangements allow them to monitor and control operational risks associated with outsourcing.</p> <p>Conduct appropriate due diligence on the financial stability, expertise and risk assessment of the Service Provider, facilities and potential debt solvency.</p> <p>consider ways to ensure a smooth transition of their business from their current agreement arrangements to a new or changed outsourcing agreement (including in the event of termination of the contract);</p> <p>Consider the impact of any concentration risk, such as the possible business continuity impact if several companies use the same service provider.</p> <p>2) Data security</p> <p>Agencies should take measures to ensure the data security of sensitive information, such as customer information, by strengthening the</p>	<p>The customer shall conduct risk analysis and due diligence before using the outsourcing service. Configure access control rules to protect sensitive user information. Have emergency plans and emergency handling processes.</p>	<p>HUAWEI CLOUD will arrange dedicated personnel to actively cooperate with financial institutions in the due diligence. To enable users to enjoy secure and reliable cloud platforms and cloud services, HUAWEI CLOUD has built a comprehensive security system in terms of security technologies, security regulations, and personnel management based on authoritative security standards around the world, and has obtained numerous security certifications at home and abroad. Huawei advocates the concept and practice of "everyone understands security" within the company,</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>management of information and communications technology-related outsourcing service providers, including:</p> <p>Ensure that there is a clear distinction between outsourced information and other information processed by the service provider.</p> <p>Service Provider employees should be authorised on a "need to know" and "minimum authorisation" basis.</p> <p>Ensure that service providers ensure that their personnel meet the required confidentiality threshold.</p> <p>Ensure that all relevant sensitive information is removed from the service provider's storage when the outsourcing arrangement is terminated.</p> <p>3) Contingency plan</p> <p>Institutions should ensure that they have appropriate contingency plans in place to deal with losses arising from significant risks to the service provider's services. Specific issues to consider include significant loss of resources, turnover of key employees, or financial distress of service providers, and unexpected termination of outsourcing agreements.</p>		<p>creating a ubiquitous, dynamic, and competitive security culture. It also runs through HUAWEI CLOUD recruitment and talent selection, employee onboarding, on-boarding training, continuous training, internal transfer, and resignation.</p> <p>HUAWEI CLOUD attaches great importance to users' data assets and regards data protection as the core of HUAWEI CLOUD security policies. HUAWEI CLOUD will continue to comply with industry-leading standards for data security lifecycle management and adopt excellent technologies, practices, and processes in</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			<p>identity authentication and access control, permission management, data isolation, transmission security, storage security, data deletion, physical destruction, and data backup and restoration. Ensure that users' privacy, ownership, and control rights over their data are not infringed, and provide users with the most effective data protection. For details, see Part 4 in HUAWEI CLOUD Data Security White Paper.</p> <p>As a cloud service provider, HUAWEI CLOUD provides financial institutions with cloud services on which their services depend. Except for outsourcing interruption or unexpected</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			<p>termination caused by force majeure, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics to continuously and effectively provide services for customers. Ensure the development of customer business. HUAWEI CLOUD conducts business continuity publicity and training in the organization every year, and regularly conducts emergency drills and tests to continuously optimize the emergency response mechanism.</p>

6

How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of IRA Risk Management and Internal Control Guidelines

The Insurance Regulatory Bureau issued the IRA Risk Management and Internal Control Standards in June 2013, which requires insurance companies to have effective risk management and internal control systems as part of the overall corporate management framework, including effective risk management, compliance, and internal audit.

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

6.1 Risk management system

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
6.0 Risk management system	<p>6.2.6 Appropriate procedures and tools (including appropriate models) for identifying, assessing, monitoring, managing and reporting risks. Such processes should also cover areas such as contingency planning, business continuity and crisis management.</p> <p>6.10 The insurance company shall be required to record major changes to the risk management system and obtain the approval of the Board of Directors. The reasons for the change shall be documented and provided to Internal Audit, External Audit and the Authority for their respective assessment of the risk management system.</p>	The customer shall require the service provider to have SLA, formulate emergency plan and business continuity plan, and ensure the availability of business.	<p>HUAWEI CLOUD provides an online version of the HUAWEI CLOUD Service Level Agreement, which specifies the content and level of services provided, as well as the responsibilities of HUAWEI CLOUD. The audit and supervision rights and interests of customers and their regulators on HUAWEI CLOUD will be agreed in the agreement signed with customers according to the actual situation. HUAWEI CLOUD has obtained ISO27001, ISO27017, ISO27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by a third party every year.</p> <p>As a cloud service provider, HUAWEI CLOUD provides financial institution customers with cloud services on which their business depends. Therefore, except for outsourcing interruption or accidental termination caused by irresistible factors, HUAWEI CLOUD has developed a business continuity management system that conforms to its own business characteristics to provide customers with continuous and effective services and ensure the development of customer business.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			HUAWEI CLOUD will conduct business continuity publicity and training in the organization every year, as well as regular emergency drills and tests, to continuously optimize the emergency response mechanism.

6.2 Risk Mitigation and Control

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
7.0 Risk Mitigation and Control	<p>7.6 When designing an effective internal control system, the insurer shall consider at least the following:</p> <p>7.6.2 Appropriate controls over other critical business processes and policies, including significant business decisions and transactions (including intra-Group transactions), critical IT functions, employee access to databases and IT systems, and significant legal and regulatory obligations.</p> <p>7.6.3 Appropriate segregation of duties shall be carried out as necessary and controls shall be put in place to ensure that such segregation is observed.</p> <p>7.6.4 A clearly defined system of management responsibilities and accountability, including documents for approval, setting limits and</p>	<p>7.6 When designing an effective internal control system, the insurer shall consider at least the following:</p> <p>7.6.2 Appropriate controls over other critical business processes and policies, including significant business decisions and transactions (including intra-Group transactions), critical IT functions, employee access to databases and IT systems, and significant legal and regulatory obligations.</p> <p>The customer requires the service provider to take strict access control measures to prevent unauthorized access and periodically check the system</p>	<p>HUAWEI CLOUD implements role-based access control and permission management for internal personnel. Personnel in different positions and responsibilities can only perform specific operations on authorized objects. Minimized permission assignment and strict behavior audit ensure that personnel do not have unauthorized access.</p> <p>HUAWEI CLOUD can cooperate with and actively respond to customer requirements. In addition, HUAWEI CLOUD has developed a comprehensive information security risk management mechanism to regularly conduct risk assessment and compliance review to ensure secure and stable running of HUAWEI CLOUD cloud environment. HUAWEI CLOUD complies with Huawei's information security risk management framework and strictly defines the risk management scope, risk management organization, and risk management process standards. Risk assessment is conducted once a year. If there are major changes to the information system, business, laws, and standards, HUAWEI</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>delegation of authority.</p> <p>7.6.7 Procedures for regularly checking that all controls as a whole form a coherent system and that the system is functioning as intended.</p> <p>7.6.8 Periodic testing and evaluation. (by objective parties such as internal or external auditors) to determine the adequacy, completeness and effectiveness of the system of internal control and its effectiveness in controlling the business of the insurance company by the board of directors and management.</p> <p>6.10 The insurance company shall be required to record major changes to the risk management system and obtain the approval of the Board of Directors. The reasons for the change shall be documented and provided to Internal Audit, External Audit and the Authority for</p>	<p>architecture, monitoring system, and pressure test mechanism to ensure service stability.</p>	<p>CLOUD will increase the number of risk assessment times. HUAWEI CLOUD implements strict security management for subcontractors and regularly audits and evaluates suppliers.</p> <p>According to the ISO27001 standard, HUAWEI CLOUD has built a comprehensive information security management system, formulated the overall information security strategy of HUAWEI CLOUD, and specified the structure and responsibilities of the information security management organization, as well as the management methods, key directions, and objectives of information security system files. include asset security, access control, cryptography, physical security, operational security, communications security, system development security, vendor management, information security incident management, and business continuity. HUAWEI CLOUD fully protects the inviolability, integrity, and availability of customers' systems and data. In addition, HUAWEI CLOUD focuses on cultivating security awareness among employees and outsourced personnel, and develops applicable security awareness training plans</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	their respective assessment of the risk management system.		and regularly conducts training.

7

How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of CBK Prudent Outsourcing Guidelines CBK PG 16

The Central Bank of Kenya issued Prudential Principles in January 2013, providing basic standards that financial institutions must implement, including CBK Prudential Outsourcing Guidelines CBK/PG/16. The fourth part of the specific requirements restricts the internal control and prudential standards, risk management practices of outsourcing financial services, regulatory and supervisory requirements, offshore outsourcing of financial services and other related security requirements.

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

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
4.5.6 Outsourcing Agreement	<p>4.5.6.1 Outsourcing arrangements shall be governed by clear written contracts, the nature and details of which shall be commensurate with the importance of outsourcing activities to the continued business of the regulated entity.</p> <p>4.5.6.6 The agreement should also indicate the nature of the legal relationship between the parties (such as agent, principal or others). The key terms of the contract should include:</p> <p>b) Organizations must ensure that they have access to all documents, records and information related to outsourcing activities of service providers.</p> <p>c) The contract should provide for the agency</p>	<p>The user agreement between the customer and the service provider shall include:</p> <p>All documents, records and information related to outsourcing activities shall be provided to financial institutions;</p> <p>The service provider shall be responsible for responding to customer data leakage;</p> <p>Financial institutions can audit service providers;</p> <p>Allow CBK to consult the necessary information provided, stored or processed by the service provider;</p> <p>Agree that CBK will arrange personnel to check the service provider and its account registered with the service provider.</p>	<p>HUAWEI CLOUD will arrange special personnel to actively cooperate with financial institutions in their due diligence. In order to enable users to enjoy a secure and reliable cloud platform and cloud services, HUAWEI CLOUD has built a complete security system from security technologies, security systems, personnel management and other aspects in accordance with authoritative security standards around the world, and has obtained numerous security certifications at home and abroad. Huawei advocates the concept and practice of "everyone understands security" within the company, creating a security culture that is everywhere, dynamic and competitive. It also runs through HUAWEI CLOUD recruitment and selection, employee</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>to continuously monitor and evaluate the service provider so that any necessary corrective action can be taken immediately.</p> <p>e) Control measures to ensure the confidentiality of customer data, and ensure that service providers should be responsible for violating security regulations and disclosing customer related confidential information.</p> <p>f) Emergency plan to ensure business continuity.</p> <p>g) The contract shall specify whether the agency approves the service provider to use subcontractors in all or part of the outsourcing activities.</p> <p>h) Provided that the Agency shall have the right to audit</p>		<p>induction, induction training, continuous training, internal transfer and resignation.</p> <p>HUAWEI CLOUD attaches great importance to users' data information assets, and regards data protection as the core of HUAWEI CLOUD's security strategy. HUAWEI CLOUD will continue to follow the industry's advanced standards for data security lifecycle management. In terms of identity authentication and access control, permission management, data isolation, transmission security, storage security, data deletion, physical destruction, data backup and recovery, HUAWEI CLOUD will adopt excellent technologies, practices and processes to ensure that users' privacy, ownership and control of their data are not violated, and provide the most</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>the Service Provider, whether by its internal or external auditors or by an agency appointed to act on its behalf externally, and the Agency shall have the right to obtain copies of any audit or review reports or findings relating to the services provided to the Agency.</p> <p>i) Provisions allowing the central bank or its authorized personnel to access the documents, transaction records and other necessary information provided, stored or processed by the service provider within a reasonable time. If such information is not provided to the Central Bank within a reasonable time, the Central Bank may take any or all remedial measures and</p>		<p>effective data protection for users. For more details, see Part 4 of HUAWEI CLOUD Data Security White Paper.</p> <p>As a cloud service provider, HUAWEI CLOUD provides financial institution customers with cloud services on which their business depends. Therefore, except for outsourcing interruption or accidental termination caused by irresistible factors, HUAWEI CLOUD has developed a business continuity management system that conforms to its own business characteristics to provide customers with continuous and effective services and ensure the development of customer business. HUAWEI CLOUD will conduct business continuity publicity and training in the organization every year, as well as regular emergency</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>administrative sanctions under the Banking Law.</p> <p>j) Make provisions recognizing that the Central Bank has the right to arrange for one or more of its officers or employees or other persons to inspect the Bank's service providers and their books and accounts.</p>		<p>drills and tests, to continuously optimize the emergency response mechanism.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
4.5.7 Confidentiality and Security	<p>The institution must ensure that the service provider's security policies, procedures and controls will enable the institution to protect the confidentiality and security of customer information. At a minimum, the institution should take the following steps to ensure that customer confidentiality issues are addressed.</p> <p>a) Access to User Information by the Service Provider's employees shall be limited to areas of information required to perform outsourced functions.</p> <p>b) Institution shall ensure that Service Providers are able to segregate and clearly identify Institution's customer information, documents, records and</p>	<p>The customer should set up access control mechanisms so that employees of the service provider can only access user information within the function.</p> <p>Service Providers should be able to segregate the institution's information files, records and other assets to protect the confidentiality of the information. The service provider shall cooperate with the organization to regularly review and check the security of the service and disclose security vulnerabilities to users in a timely manner.</p>	<p>HUAWEI CLOUD attaches great importance to users' data assets and regards data protection as the core of HUAWEI CLOUD security policies. HUAWEI CLOUD will continue to comply with industry-leading standards for data security lifecycle management and adopt excellent technologies, practices, and processes in identity authentication and access control, permission management, data isolation, transmission security, storage security, data deletion, physical destruction, and data backup and restoration. Ensure that users' privacy, ownership, and control rights over their data are not infringed, and provide users with the most effective data protection. For more details, see Part 4 in HUAWEI CLOUD Data Security White Paper.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>assets to protect the confidentiality of information.</p> <p>c) The Agency shall periodically review and monitor the Service Provider's security practices and control procedures and require the Service Provider to disclose security vulnerabilities.</p>		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
4.5.8 Business Continuity Management	<p>The institution should take steps to assess and ensure that the risks of interdependence arising from outsourcing arrangements are sufficiently mitigated to enable the institution to conduct its business with integrity and competence in the event of a business interruption, unexpected termination of outsourcing or liquidation of a service provider.</p> <p>a) Agencies require their service providers to develop and establish a robust framework to document, maintain and test business continuity and recovery procedures. Organizations need to ensure that service providers regularly test business continuity and recovery plans, or may consider conducting joint</p>	<p>The customer shall require the service provider to develop the BCP and conduct emergency drills irregularly.</p> <p>The Customer should ensure that the Service Provider is able to segregate the Agency's information files, records and other assets; Ensure that the documents and records submitted to the service provider can be recovered from the service provider, deleted, destroyed, and unusable for the continued operation of the organization's business.</p>	<p>As a cloud service provider, HUAWEI CLOUD provides financial institutions with cloud services on which their services depend. Except for outsourcing interruption or unexpected termination caused by force majeure, HUAWEI CLOUD has developed a business continuity management system that meets its business characteristics to continuously and effectively provide services for customers. Ensure the development of customer business. HUAWEI CLOUD conducts business continuity publicity and training in the organization every year, and regularly conducts emergency drills and tests to continuously optimize the emergency response mechanism.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>test and recovery exercises with their service providers from time to time.</p> <p>d) Outsourcing usually requires a shared service provider's infrastructure. The institution should ensure that the service provider is able to segregate the institution's information, documents and records, and other assets. This is to ensure that, under adverse conditions, all documents, transaction records and information to the service provider, as well as the assets of the institution, can be removed from the service provider to continue its business operations, or deleted, destroyed or rendered unusable.</p>		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
4.5.9 Monitoring and control of outsourced activities	<p>4.5.9.1 The institution shall establish a management structure to monitor and control its outsourced activities</p> <p>4.5.9.2 As outsourcing relationships and interdependencies increase in importance and complexity, a more rigorous approach to risk management should be adopted.</p> <p>4.5.9.4 Institutions should ensure that outsourcing agreements with service providers contain provisions addressing the oversight and control of their outsourcing activities.</p> <p>4.5.9.5 Structures for effective monitoring and control of material outsourcing will include the following:</p> <p>c) The Agency shall review the</p>	<p>The client should establish outsourcing management procedures, risk management of outsourcing activities, ensure that outsourcing agreements with the service provider contain provisions addressing oversight and control of its outsourcing activities, and conduct due diligence on the service provider at least once a year.</p>	<p>HUAWEI CLOUD provides an online version of the HUAWEI CLOUD Service Level Agreement, which specifies the content and level of the services provided and HUAWEI CLOUD's responsibilities. The audit and supervision rights of the customer and its regulatory authorities on HUAWEI CLOUD will be specified in the agreement signed with the customer based on the actual situation. HUAWEI CLOUD has obtained international security and privacy protection certifications such as ISO27001, ISO27017, ISO27018, SOC, and CSASTAR, and is audited by a third party every year.</p> <p>HUAWEI CLOUD will arrange dedicated personnel to actively cooperate with financial institutions in the due diligence. To enable users to enjoy secure and reliable cloud platforms and</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	financial and operational status of the Service Provider at least annually to assess its ability to continue to provide the Outsourced Services. Such due diligence could be based on all available information about the service provider and should highlight areas such as violations of performance standards, confidentiality and security, and business continuity preparedness.		cloud services, HUAWEI CLOUD has built a comprehensive security system in terms of security technologies, security regulations, and personnel management based on authoritative security standards around the world, and has obtained numerous security certifications at home and abroad.

8

How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of GUIDANCE NOTE ON CYBERSECURITY

The Insurance Regulatory Bureau issued the IRA Risk Management and Internal Control Standards in June 2013, which requires insurance companies to have effective risk management and internal control systems as part of the overall corporate management framework, including effective risk management, compliance, and internal audit.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
3.3 Outsourcing	<p>The outsourcing agreement shall be properly managed, including due diligence on potential service providers, signing of written outsourcing agreements and proper supervision on the provision of services.</p> <p>Select suppliers based on compliance and risk assessment.</p> <p>Ensure the security of all computing resources, including registration, licensing, compliance and verification.</p> <p>Ensure that all outsourcing contracts require service providers to comply with applicable legal and regulatory frameworks.</p> <p>Understand the inherent risks of each third party.</p> <p>Analyze the outsourcing portfolio of the institution to understand which pose the greatest relative risks to the institution.</p>	<p>The customer shall conduct due diligence on the service provider, properly supervise the outsourcing service, and ensure that the service provider meets the compliance requirements.</p> <p>Ensure the security of computing resources used by service providers (for example, software and hardware are genuine); Ensure that outsourcing contracts specify that service providers comply with local regulations and meet regulatory requirements.</p>	<p>In order to cooperate with customers to exercise supervision over cloud service providers, HUAWEI CLOUD User Agreement on HUAWEI CLOUD Online divides security responsibilities between customers and Huawei. HUAWEI CLOUD Cloud Service Level Agreement specifies the service level provided by HUAWEI CLOUD. At the same time, HUAWEI CLOUD has also developed offline contract templates, in which corresponding requirements can be jointly agreed with customers according to their requirements. For more details, please refer to HUAWEI CLOUD User Agreement.</p> <p>HUAWEI CLOUD provides an online version of the HUAWEI CLOUD Service Level Agreement, which specifies the content and level of services provided, as well</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			<p>as the responsibilities of HUAWEI CLOUD. HUAWEI CLOUD will arrange special personnel to actively cooperate with financial institutions in their due diligence. The audit and supervision rights and interests of customers and their regulators on HUAWEI CLOUD will be agreed in the agreement signed with customers according to the actual situation. HUAWEI CLOUD has obtained ISO27001, ISO27017, ISO27018, SOC, CSA STAR and other international security and privacy protection certifications, and is audited by a third party every year.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
4.0 Reporting	b) Each institution shall notify the Central Bank of Kenya within 24 hours of any cybersecurity incident which may materially and adversely affect the institution's ability to provide appropriate services to its clients, its reputation or its financial position.	If a financial institution encounters a cyber security incident, which has a significant adverse impact on its service capability, financial status, and reputation, the financial institution shall report the incident to the Central Bank of Kenya within 24 hours.	HUAWEI CLOUD reviews and summarizes the impact of security incidents and the handling process, and notifies and reports the impacted users and supervision departments as required. HUAWEI CLOUD has developed a comprehensive event management and customer notification process. If an event occurs on the underlying platform of HUAWEI CLOUD, related personnel will analyze the impact of the event based on the process. If the event has or will affect cloud service customers, HUAWEI CLOUD will start the notification mechanism. Notify the customer of the event. The notification content includes but is not limited to the incident description, cause, impact, measures taken by HUAWEI CLOUD, and measures recommended by the customer.

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			To meet customers' requirements for reporting cyber security incidents, HUAWEI CLOUD sets up a 24/7 professional security incident response team and expert resource pool to disclose related incidents in a timely manner and notify customers in a timely manner according to laws and regulations. In addition, HUAWEI CLOUD implements emergency plans and recovery processes to reduce service impact.

9

How HUAWEI CLOUD Meets and Assists Customers to Meet Implementation of Internet Security Guide for Payment Service Providers

The Central Bank of Kenya issued the Guidelines on Network Security of Payment Service Providers in November 2019, setting the minimum standards that payment service providers (PSPs) should adopt to develop an effective network security governance and risk management framework.

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

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
3.2.4 Incident Response and Network Resilience	<p>(ii) The PSP shall enhance its cyber resilience by planning, responding to, controlling and being able to recover rapidly from the disruption caused by a cyber incident. As a result, PSPs should have the ability to operate critical business functions in the face of an attack while continuously enhancing cyber resilience. The following aspects should be addressed:</p> <p>a) Internal processes for responding to cybersecurity incidents.</p> <p>b) Objectives of the incident response plan.</p> <p>c) Clear definition of roles, responsibilities, and levels of decision-making authority.</p> <p>d) External and internal communication and information sharing.</p> <p>e) Identify requirements for</p>	<p>The PSP shall have an emergency response plan to improve the emergency response and handling capability of information security incidents and enhance the emergency response capability. The contingency plan should include descriptions of the cyber security incident handling process, response plan, personnel roles, and responsibilities.</p>	<p>HUAWEI CLOUD standardizes the emergency response process and formulates emergency response plans based on different emergency scenarios that may be involved in each product. In addition, HUAWEI CLOUD conducts business continuity publicity and training in the organization every year, and regularly conducts emergency drills and tests to continuously optimize the emergency response mechanism. HUAWEI CLOUD provides training and testing on information security incident management procedures and processes every year. All security incident response personnel, including backup personnel, must participate in the training.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>remediation of any identified weaknesses in the information system and related controls.</p> <p>f) record and report on cybersecurity incidents and related incident response activities;</p> <p>g) After a cyber security incident occurs, evaluate and revise the incident response plan as necessary.</p>		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
3.2.5 Vulnerability Assessment and Penetration Testing	<p>Each PSP's cybersecurity plan shall include monitoring and testing, developed based on the PSP's risk assessment, with the aim of assessing the effectiveness of the PSP's cybersecurity plan. Monitoring and testing should include ongoing monitoring and periodic penetration testing and vulnerability assessment. In the absence of effective continuous monitoring, or other systems that continuously detect changes in the information system that may produce or indicate vulnerabilities, PSP's shall proceed.</p> <p>(i) Vulnerability scans of all critical network assets on a quarterly basis.</p> <p>(ii) the PSP's annual penetration testing, covering</p>	<p>PSPs should continuously monitor business systems and conduct regular penetration testing and vulnerability scanning.</p> <p>1) Vulnerability scan for important service systems/assets on a quarterly basis.</p> <p>2) Penetration tests are conducted on important business systems/assets every year.</p> <p>3) Vulnerability assessment of the information system, including host scanning and web scanning, is conducted every six months.</p>	<p>HUAWEI CLOUD has established management regulations on penetration testing and vulnerability scanning, which specify the purpose, frequency, and security requirements for penetration testing on HUAWEI CLOUD, standardize penetration testing activities, and ensure that penetration testing activities are compliant and controlled.</p> <p>HUAWEI CLOUD organizes qualified third parties to perform penetration tests on all systems and applications on the Huawei cloud platform every six months, and tracks and rectifies the penetration test results. Penetration test reports and follow-up are verified by internal audits and external certification bodies.</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>at least the critical network assets identified annually based on the risk assessment</p> <p>(iii) a semi-annual vulnerability assessment, including any system scan or review of the Information System, reasonably designed to identify publicly known cybersecurity vulnerabilities in the PSP Information System based on the risk assessment.</p>		

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
3.4 Outsourcing	<p>(i) Establish an appropriate outsourcing agreement management framework, including conducting due diligence on potential service providers, signing written outsourcing agreements, and fully monitoring service delivery.</p> <p>(iv) Ensure that all outsourcing contracts require service providers to comply with applicable legal and regulatory frameworks.</p> <p>(vii) mandatorily require its outsourcers to report security incidents/ violations within a specific time frame consistent with best practice. It is usually limited to 48 hours.</p> <p>(viii) Ensure that outsourced services or infrastructure meet at least the same minimum security standards as PSP's non outsourced</p>	<p>The customer shall conduct due diligence on the service provider, properly supervise the outsourcing service, and ensure that the service provider meets the compliance requirements; And meet the minimum security standards of PSP non outsourcing services.</p> <p>In case of a security incident, the service provider shall report it within 48 hours.</p> <p>Ensure that outsourcing contracts specify that service providers comply with local regulations and meet regulatory requirements; Ensure that the SLA has clear penalties:</p> <p>PSP and CBK's right to audit service providers and penalty clauses for security incidents; Responsibilities of service providers in case of security problems and disclosure of customer related confidential information.</p> <p>Details of outsourcing activities, including appropriate services and performance standards.</p> <p>Emergency plan to ensure business continuity.</p> <p>Provisions allowing the CBRC or its authorized personnel to check the institution's documents, transaction records and other necessary</p>	<p>HUAWEI CLOUD will arrange special personnel to actively cooperate with financial institutions in their due diligence. In order to enable users to enjoy a secure and reliable cloud platform and cloud services, HUAWEI CLOUD has built a complete security system from security technologies, security systems, personnel management and other aspects in accordance with authoritative security standards around the world, and has obtained numerous security certifications at home and abroad. Huawei advocates the concept and practice of "everyone understands security" within the company, creating a security culture that is everywhere, dynamic and competitive. It also runs through HUAWEI CLOUD recruitment and selection, employee induction, induction training, continuous training, internal transfer and resignation.</p> <p>As a cloud service provider, HUAWEI CLOUD provides financial institution customers with cloud</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
	<p>services and infrastructure.</p> <p>(ix) Ensure that the service level agreement fully contains provisions on security, service availability, performance indicators and penalties.</p>	<p>information provided, stored or processed by the service provider within a reasonable time</p>	<p>services on which their business depends. Therefore, except for outsourcing interruption or accidental termination caused by irresistible factors, HUAWEI CLOUD has developed a business continuity management system that conforms to its own business characteristics to provide customers with continuous and effective services and ensure the development of customer business. HUAWEI CLOUD will conduct business continuity publicity and training in the organization every year, as well as regular emergency drills and tests, to continuously optimize the emergency response mechanism.</p> <p>In order to cooperate with customers to exercise supervision over cloud service providers, HUAWEI CLOUD User Agreement on HUAWEI CLOUD Online divides security responsibilities between customers and Huawei. HUAWEI CLOUD Cloud Service Level Agreement specifies</p>

No.	Control Principle	Customers Considering	HUAWEI CLOUD Response
			the service level provided by HUAWEI CLOUD. At the same time, HUAWEI CLOUD has also developed offline contract templates, in which corresponding requirements can be jointly agreed with customers according to their requirements. For more details, please refer to HUAWEI CLOUD User Agreement .

10 Conclusion

This article describes how HUAWEI CLOUD provides customers with cloud services that comply with the regulatory requirements of the financial industry in Kenya, and shows that HUAWEI CLOUD complies with the key regulatory requirements issued by the Central Bank of Kenya, which helps customers to understand in detail HUAWEI CLOUD's compliance with the regulatory requirements of the financial industry in Kenya, so that customers can safely and confidently store and process customer content data through HUAWEI CLOUD services. At the same time, to some extent, this article also guides customers on how to design, build and deploy a secure cloud environment that complies with the regulatory requirements of Kenya's financial industry on HUAWEI CLOUD, and helps customers better share the corresponding security responsibilities with HUAWEI CLOUD.

This white paper is for general reference only and does not have any legal effect or constitute any form of legal advice. The customer should assess his own use of cloud services at his discretion and be responsible for ensuring compliance with the regulatory requirements of the financial industry in Kenya when using HUAWEI CLOUD.

11

Version History

Date	Version	Description
February 2023	1.0	First release