HUAWEI CLOUD Security Companion Guide for Cyber Security Agency of Singapore (CSA) Cyber Trust mark certification

Issue **1.0**

Date **2024-10-16**

CSA SINGAPORE

SG CYBER SAFE

CYBER TRUST

HUAWEI

Trademarks and Permissions


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

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

Notice

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

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

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

Increasingly digital lifestyles also increase the cyber risks faced by organizations and individuals. Cybersecurity has become a key enabler of Singapore's digital economy. In this context, Cyber Security Agency of Singapore (CSA) released a framework which describes tiered cybersecurity standards to support the cybersecurity needs of a range of organizations on 29 March 2022.

CSA Releases tiered cybersecurity standards for enterprises consists of the main text and two annexes. In the main text, the CSA introduces organizations to the risk assessment methodology for identifying organizational cybersecurity management boundaries and identifying organizational cybersecurity risks. Also, considering that organizations differ in the nature, size and digitalization of their business, which has a corresponding impact on their cybersecurity risk profile, CSA has adopted a tiered approach in cybersecurity standards to provide a guided approach to help organizations in their journey towards the implementation of cybersecurity in the organization. The cybersecurity measures are presented in Annex A and Annex B as follows:

- Annex A: Cyber Essentials mark, which takes a baseline control approach and is designed to protect organizations from the most common cyber-attacks;
- Annex B: Cyber Trust mark takes a risk-based approach and is designed to enable organizations to implement relevant cybersecurity preparedness measures commensurate with their cybersecurity risk profile.

Together, the Cyber Essentials mark and the Cyber Trust mark provide a framework for cyber security risk management for organizations.

For details information of Cyber Essentials mark and the Cyber Trust mark, please refer to CSA website: www.csa.gov.sg/cyber-certification.

1.2 Basic Definitions

- **HUAWEI CLOUD**

  HUAWEI CLOUD is the cloud service brand of the HUAWEI marquee, committed to providing stable, secure, reliable, and sustainable cloud services.
- **Customer (Tenant)**

Refers to the registered users who build business relationships with HUAWEI CLOUD. In this whitepaper, customers have the same meaning of tenant which indicates the user organization that use the services provided by HUAWEI CLOUD. The term “tenant” is used in some scenarios in this document.

- **Business-critical data**

  Data within the organization such as product, staff and financial data that is vital to the operation of the organization; where losing or exposing them can lead to detrimental impact, e.g., potential financial loses and legal issues.

- **Certification body**

  In the context of Cyber Essentials and Cyber Trust mark, certification body refers to an organization that has appointed by CSA to provide conformity assessment and to issue certificates of the marks.

- **Cloud shared responsibility model**

  The cloud shared responsibility model is a security framework used to ensure a common understanding of the security responsibilities shared between a cloud provider and its consumer.

- **Cyber hygiene**

  Cyber hygiene is a practice in cybersecurity to maintain and protect an organization’s systems from threat through adopting basic cyber health and security postures. It should be commensurate with the business activities of the organization, with its associate risks.

- **Passphrase**

  Passphrase is typically a longer form of password that use a combination of random words, rather than just characters.

- **Use of “shall” and “should”**

  In this standard, the following verbal forms are used:

  - “shall” indicates a requirement;
  - “should” indicates a recommendation;
  - “may” indicates a permission;
  - “can” indicates a possibility or a capacity.

- **CSA CCM**

  Cloud Security Alliance Cloud Control Matrix is the world's only meta-framework of cloud-specific security controls mapped to leading standards, best practices and regulations.

- **CSA CAIQ**

  The Consensus Assessments Initiative Questionnaire (CAIQ) offer an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services, providing security control transparency. It provides a set of Yes/No questions a cloud customer and cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the Cloud Controls Matrix (CCM).

- **CSA STAR Certification**

  An authoritative certification for cloud security level launched by the CSA and the BSI together, where STAR is the abbreviation for Security, Trust, Assurance and Risk. The certification is evaluated and audited based on the requirements of CSA CCM and ISO 27001.

- **ISO 27001 Information Security Management System**

  ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this

standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls. ISO 27002 is the best practices based on ISO 27001.

- **ISO 27017 Cloud Service Information Security Management System**

  ISO 27017 is the practical rules for cloud service information security control based on the ISO 27001 system framework and ISO 27002 best practices. It is an international implementation procedures standard for cloud service information security control.

- **ISO 27701 Privacy Information Management System**

  As a privacy extension to ISO 27001 and ISO 27002, ISO 27701 is an authoritative international standard of privacy management field. ISO 27701 specifies requirements and guidance for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS) and its relevant content.

- **ISO 22301 Business Continuity Management System**

  ISO 22301 is an international standard for business continuity management systems. ISO 22301 help organizations avoid potential incidents through identifying, analyzing and warning of risk, and formulate a complete business continuity plan to effectively respond to quick recovery after interruption and maintain normal running of core functions and minimize loss and recovery costs.

- **SOC Audit Reports**

  The SOC audit reports are independent audit reports designed by a third-party audit institution based on relevant standards formulated by the American Institute of Certified Public Accountants (AICPA) for the system and internal control of outsourced service providers.

- **NIST Cybersecurity Framework**

  The NIST cyber security framework consists of three parts: standards, guidelines, and best practices for managing cyber security risks. The core content of the framework can be summarized as the classic IPDRR capability model namely the five capabilities: Identify, Protect, Detect, Response and Recovery.

1.3 Document Scope

There are three (3) main types of cloud computing service models: (i) Software-as-a-Service (SaaS), (ii) Infrastructure-as-a-Service (IaaS) and (iii) Platform-as-a-Service (PaaS).

This cloud security companion guide is intended for end-user organizations that are infrastructure as a service (IaaS) users and have implemented or are preparing to implement security measures from the Cyber Trust mark to help users understand:

- As a cloud service provider, this document aims to help its customers understand how HUAWEI CLOUD services and tools can be used to address the cybersecurity preparedness domains in Cyber Trust mark.

The relationship between this cloud security companion guide and the cyber security certification documents released by CSA is as follows:

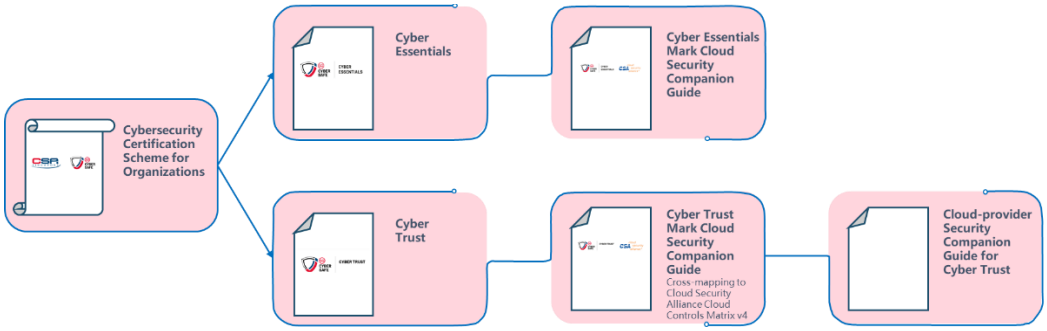


Figure 1-1 Supplementary documents for CSA cyber security certification

- Cybersecurity Certification Scheme for Organizations: Cybersecurity Essentials Mark and Cybersecurity Trust Mark;
- Cyber Essentials: document outlining the Cyber Essentials cybersecurity certification standard, published as a national standard in Singapore;
- Cyber Trust mark: This document outlines Cyber Trust's cyber security certification standards and is published as a national standard in Singapore.
- Cloud Security Companion Guide for Cyber Essentials: an implementation guide to accompany the Cyber Essentials mark certification document, targeted at organizations that are cloud users who are implementing or preparing to implement the security measures in the Cyber Essentials mark;
- Cloud Security Companion Guide for Cyber Trust: Cross-mapping between CSA Cyber Trust and Cloud Security Alliance Cloud Controls Matrix v4;
- Cloud-provider Security Companion Guide for Cyber Trust: HUAWEI CLOUD Security Companion Guide for Cyber Security Agency of Singapore (CSA) Cyber Trust.

2 The Certification Status of HUAWEI CLOUD

With its own cyber security system and security control management, HUAWEI CLOUD has obtained the CSA Cyber Trust mark (Advocate) tier certification. The certification covers products and services released by HUAWEI CLOUD on its official website, as well as data centers around the world.

For details about the certification scope and activity of Cyber Trust mark, see the certificate of registration available on HUAWEI CLOUD **Trust Center- 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:

Regional standard certification for Singapore

Certification	Description
Singapore Multi-Tier Cloud Security (MTCS) Level 3 Certification	The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to implement sound risk management and security practices for cloud computing. Huawei Cloud has earned MTCS level 3 certification.
OSPAR Certification	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 Certification the ABS Guidelines.
CSA Cyber Trust mark (Advocate) tier Certification	The Cyber Trust mark is a cybersecurity certification for organisation, developed by CSA. This certification takes a risk-based approach and is designed to enable organizations to implement relevant cybersecurity preparedness measures commensurate with their cybersecurity risk profile. Currently, HUAWEI CLOUD has obtained the (Advocate) tier certification, the highest level of Cyber Trust mark.

Global standard certification

Certification	Description
ISO27001	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.
ISO27017	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.
ISO27018	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.
TL 9000& ISO 9001	ISO 9001 defines a set of core standards for quality management systems (QMS). It can be used to certify that an organization has the ability to provide products that meet customer needs as well as applicable regulatory requirements. TL 9000 is a quality management system built on ISO 9001 and designed specifically for the communications industry by the QuEST Forum (a global association of ICT service providers and suppliers). It defines quality management system specifications for ICT products and service providers and includes all the requirements of ISO 9001. Any future changes to ISO9001 will also cause changes to TL 9000. Huawei Cloud has earned ISO 9001/TL 9000 certification, which certifies its ability to provide you with faster, better, and more cost-effective cloud services.
ISO 20000-1	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.
ISO22301	ISO 22301 is an internationally recognized business continuity management system standard that helps organizations avoid potential incidents by identifying, analyzing, and alerting risks, and develops a comprehensive Business Continuity Plan (BCP) to effectively respond to disruptions so that entities can recover rapidly, keep core business running, and minimize loss and recovery costs.
CSA STAR Certification	The Cloud Security Alliance (CSA) and the British Standards Institution (BSI), an authoritative standard development and preparation body as well as a worldwide certification service provider, developed CSA STAR certification. This certification aims to increase trust and transparency in the cloud computing industry and enables cloud computing

Certification	Description
	service providers to demonstrate their service maturity.
ISO27701	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	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.
ISO29151	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.
PCI DSS	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.
ISO 27799	ISO/IEC 27799 provides guidelines on how organizations in the healthcare industry can better protect the confidentiality, integrity, traceability, and availability of personal health information. Huawei Cloud is the world's first cloud service provider to earn ISO/IEC 27799 certification. This certifies Huawei Cloud's deep understanding of intelligent applications for the healthcare industry, and its ability to protect the security of personal health information.
ISO 27034	ISO/IEC 27034 is the first ISO standard for secure programs and frameworks. It clearly defines risks in application systems and provides guidance to assist organizations in integrating security into their processes. ISO/IEC 27034 provides a way for organizations to verify their own product security and make security a competitive edge. This standard also outlines a compliance framework at the application layer for global cloud service providers, promoting the security of the R&D process, applications, and the cloud. Huawei Cloud is the world's first cloud service provider to obtain ISO/IEC 27034 certification. This marks a big step forward for Huawei Cloud governance and compliance.
SOC Audit Report	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.

The Cyber Trust mark, CSA STAR certification, and CSA CCM 4.0 Cloud Control Matrix v4 all refer to the ISO27001:2013 standard released by the ISO in terms of setting control domains and cybersecurity measures. The granularity and height of cyber security requirements are highly overlapped.

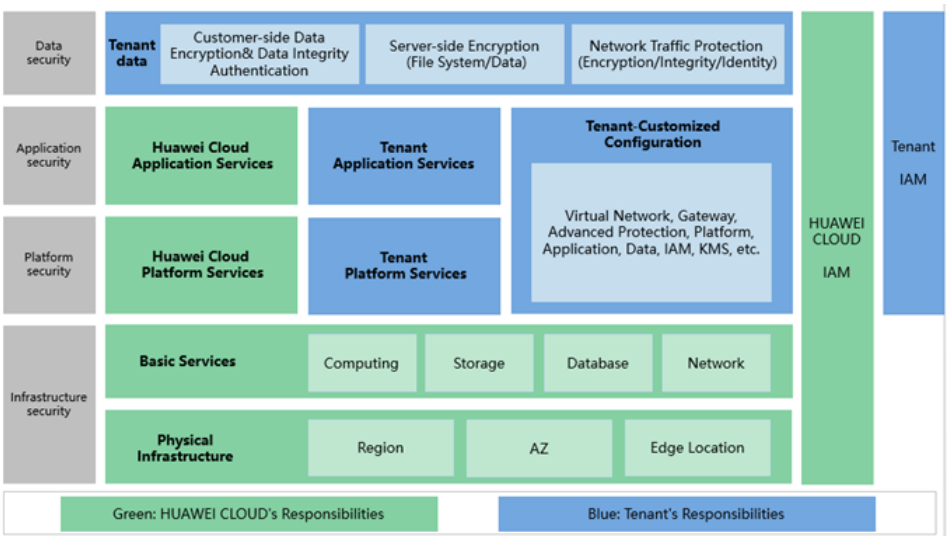
According to the Cloud Security Companion Guide for Cyber <Cross-mapping between CSA Cyber Trust and Cloud Security Alliance Cloud Controls Matrix v4>, which published by Cloud Security Alliance and CSA: Cyber Trust mark covers 70.1% of the cybersecurity measures in CSA CCM 4.0 standard.

HUAWEI CLOUD has passed the CSA STAR certification released by the Cloud Security Alliance and released the compliance instruction **<HUAWEI CLOUD Compliance with CSA CCM>**. 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 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:

图3-1 **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-tiered 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 service 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 Tenants/Customers and HUAWEI CLOUD, please refer to the **HUAWEI CLOUD Security White Paper** released by HUAWEI CLOUD.

4 HUWAEI CLOUD Helping Customers Respond to Cyber Trust mark Requirements

HUAWEI CLOUD has passed the Cyber Trust mark certification and provides customers with secure and reliable cloud services. However, this does not mean that customers' use of HUAWEI CLOUD services will automatically translate to customers meeting the cybersecurity measures in Cyber Trust mark by default.

If customers want to gain Cyber Trust mark certification, they should establish, implement, maintain and continually improve their organization's cybersecurity management system in accordance with the Cyber Trust mark cybersecurity measures, and engage a third-party independent certification body to assess it.

In this chapter, HUAWEI CLOUD provides the following functions:

(1) Guidance and mapping that aligns the security features or best practices of its own services/products with the applicable domains and measures listed in the Cyber Trust mark;

(2) Interpretation of the best practices or responsibilities of the Cyber Trust mark.

It is intended to provide customers with an understanding of how to comply and what HUAWEI CLOUD services and tools can be used to help meet the cybersecurity measures set out in Cyber Trust mark.

4.1 Cloud Security Companion Guide of Cyber Trust mark

The construction of network security management system needs to start from two aspects: management and technology. At a management level, customers should develop cybersecurity policies and procedures that meet their needs and meet the requirements of the Cyber Trust mark. At the technical level, HUAWEI CLOUD provides products and services to help customers build their own cyber security management systems in some control domains.

This Chapter starts from section B.8 (does not address requirements for organizational governance, security policies, procedures or human resource controls, specifically B.1 - B.7) and describe how products and services provided by HUAWEI CLOUD help customers build their own network security systems. Sections B.1 to B.7 are the responsibilities of tenants. For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. HUAWEI CLOUD provides some compliance documents/white papers for customers for reference.

4.1.1 Cloud Security Guidance for Governance/Policy Requirements

B.1 Governance

The objective of this domain is to ensure that the organization has practices in place to ensure that senior management is involved in the cybersecurity governance of the organization. This includes overseeing the development and implementation of a cybersecurity strategy and roadmap to ensure that goals/objectives are defined and regularly tracked.

- B.1.1 & B.1.2: No assessment domains are required for Tier 1/2 supporters and practitioners.
- B.1.3: Tier 3 Promoter need to implement cyber security practices and communicate them to the organization's stakeholders.
- B.1.4 – B.1.6: Tier 4 Performer require management to have sufficient cyber security awareness and participate in the development and implementation of the organization's cyber security strategy, guidelines, policies, procedures, and reviews.
- B.1.7 & B.1.8: The Tier 5 Advocate needs to establish a cyber security committee/forum at the management level or the Board of Directors to discuss and make decisions on the organization's cyber security plans and issues, and supervise and make decisions on the execution of cyber security policies and the organization's cyber security risks.

For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. The following is the compliance document/white paper released by HUAWEI CLOUD for tenants.

<HUAWEI CLOUD Compliance with CSA CCM> 3.8 Governance, Risk and Compliance & 3.9 Human Resource Security

B.2 Policies and procedure

The objective of this domain is to ensure that cybersecurity policies and standards are established, implemented and communicated so that employees have clear direction and guidance on secure practices to protect the organization’s environment. Formalized policies and

procedures also enable continuous review and update, monitoring for non-compliance and management involvement, to protect the organization from the evolving cyber threat landscape.

- B.2.1 & B.2.2: No assessment domains are required for Tier 1/2 supporters and practitioners.
- B.2.3: Tier 3 Promoter need to refer to industry practices or standards to regularly update the organization's cyber security policies and processes.
- B.2.4 – B.2.6: Tier 4 Performer are required to establish systematic and documented policies and procedures for risk management and asset management, and communicate and guide employees.
- B.2.7 – B.2.9: The Tier 5 Advocate shall establish a process for implementing cyber security policies and procedures, report to the BOD on the effectiveness and deviations of the implementation of cyber security policies and procedures on an annual basis, and monitor the violation or non-compliance of policies and procedures for timely rectification.

For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. The following is the compliance document/white paper released by HUAWEI CLOUD for tenants.

<HUAWEI CLOUD Compliance with CSA CCM> 3.1 Audit and assurance & 3.8 Governance, Risk and Compliance & 3.9 Human Resource Security

B.3 Risk Management

The objective of this domain is to ensure that the organization has established risk management practices in place to identify, assess, mitigate, monitor and report cybersecurity risks.

- B.3.1 & B.3.2: Tier 1 supporter need to identify cyber security risks and give priority to resolving cyber security risks of key services.
- B.3.3 & B.3.4: Tier 2 practitioners need to develop risk management plans and regularly identify and track risks.
- B.3.5 & B.3.6: Tier 3 Promoter need to establish a risk assessment process and a risk register to track risk rectification.
- B.3.7 – B.3.9: Tier 4 Performer establish risk management policies and procedures, assign risk management roles and responsibilities, and determine the organization's risk appetite and tolerance.

B.3.10 – B.3.12: The Tier 5 Advocate need to establish a cybersecurity risk management framework, review risk management deviations, and regularly report identified cybersecurity risks to the board/management.

For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. The following is the compliance document/white paper released by HUAWEI CLOUD for tenants.

<HUAWEI CLOUD Compliance with CSA CCM> 3.8 Governance, Risk and Compliance

B.4 Cyber Strategy

The objective of this domain is to ensure that the organization has established a cybersecurity strategy supported by a detailed roadmap and workplan so it can achieve planned targets and objectives over a time period and remain cyber resilient organization-wide.

- B.4.1 – B.4.4: Tier 1 to Tier 4 do not need to assess this area, but organizations should consider the content in CSA's Cybersecurity Toolkit to develop cybersecurity leadership among SMB owners, organizational leaders, and IT teams.
- B.4.5 – B.4.9: The Tier 5 Advocate need to develop organization-level cyber security strategies, implement work plans based on the strategies, and review and update the strategies every year. In addition, the board/management of the organization needs to provide sufficient budget and financial support for the cyber security strategy, and regularly evaluate and follow up the implementation and progress of the cyber security strategy every year.

For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. The following is the compliance document/white paper released by HUAWEI CLOUD for tenants.

<HUAWEI CLOUD Compliance with CSA CCM> 3.3 Business Continuity Management and Business Resilience & 3.8 Governance, Risk and Compliance

<HUAWEI CLOUD Practical Guide for NIST CSF> ID.BE-2 & RS.IM-2

B.5 Compliance

The objective of this domain is to ensure that the organization is aware of applicable laws, regulations and guidelines related to cybersecurity, so that compliance can be achieved. A compliance policy with active identification of non-compliance allows the organization to manage the associated risks.

- B.5.1: Tier 1 supporter need to identify and comply with business-related laws, regulations, guidelines, or industry standards.
- B.5.2: Tier 2 practitioners need to develop and implement compliance measures for the identified relevant laws, regulations, and guidelines.
- B.5.3 & B.5.4: Tier 3 Promoter need to communicate business-related laws, regulations, or standard guide requirements to relevant parties in the organization, and develop the compliance document update process.
- B.5.5 & B.5.6: Tier 4 Performer are required to establish and implement compliance policies and processes that comply with or address applicable legal and regulatory standards and guidelines, and assign roles and responsibilities for compliance tasks.
- B.5.7 – B.5.9: The Tier 5 Advocate need to ensure that the organization's processes and systems are legal and compliant, take measures to prevent violations of laws and regulations, and regularly report to the board of directors/management on the organization's compliance work and violations.

For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. The following is the compliance document/white paper released by HUAWEI CLOUD for tenants.

<HUAWEI CLOUD Security White Paper> 2 Cloud Security Strategy & 4.1 Security Compliance and Standards Compliance & 5.3 Internal Audit Personnel & 5.4.2 Cyber Security Capability Improvement

B.6 Audit

The objective of this domain is to ensure that the organization has established an audit program to assess the effectiveness of policies, processes, procedures and controls against cybersecurity risks.

- B.6.1 – B.6.3: Tier 1 to Tier 3 do not need to assess this area.
- B.6.4 – B.6.6: Tier 4 Performer need to develop and implement a cybersecurity audit program and establish an internal audit function or team to conduct audits of cybersecurity policies, processes, procedures, and controls. Also, develop audit remediation policies, processes and procedures.
- B.6.7 & B.6.8: The Tier 5 Advocate need to monitor and review the audit results on a quarterly basis, and report and follow up the audit results to the Board of Directors/management in a timely manner.

For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. The following is the compliance document/white paper released by HUAWEI CLOUD for tenants.

<HUAWEI CLOUD Security White Paper> 2 Cloud Security Strategy & 5.3 Internal Audit Personnel & 5.4.2 Cyber Security Capability Improvement & 9.3.1 Log Management and Audit & 9.3.2 Fast Fault Detection and Demarcation.

<HUAWEI CLOUD Compliance with ISO 27001> A.5.1Policies for information security.

B.7 Training and Awareness

The objective of this domain is to ensure that the organization has instilled cybersecurity awareness and culture among its employees so that they do not form the weakest link in the organization’s defense.

- B.7.1 – B.7.3: Tier 1-Tier 2 need to implement the cyber security suggestions under A.1 Assets: People in Cyber Essentials mark to ensure that employees have the security knowledge and awareness to identify and mitigate cyber threats. For details, see section 5.1 in this guide.
- B.7.4 & B.7.5: Tier 3 Promoter need to use metrics (e.g., attendance) to ensure employee completion of awareness training and evaluate employees after training. In addition, appoint cyber security awareness training specialists/advocates to promote cyber security awareness within the organization.

- B.7.6 – B.7.8: Tier 4 Performer shall develop cyber security awareness training policies and procedures to guide the organization in providing cyber security awareness training for all personnel (including the board of directors/management) and regularly update the training content.
- B.7.9 – B.7.11: The Tier 5 Advocate need to evaluate the effectiveness of cybersecurity awareness and training programs and conduct regular skills gap analyses. The entire cybersecurity training program needs to have a department (e.g., human resources (HR), a team within a business unit) responsible for implementation and review.

For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. The following is the compliance document/white paper released by HUAWEI CLOUD for tenants.

<HUAWEI CLOUD Security White Paper> 5.4.1 Security Awareness Education & 5.4.2 Security Competency & 5.4.3 Key Position Management

B.11 Bring Your Own Device (BYOD)

The objective of this domain is to ensure that the use of personal devices is managed securely when connected to the organization's network. This domain also addresses processes to prevent the disclosure and loss of the organization's business-critical data through personal devices.

- B.11.1 – B.11.3: Tier 1 to Tier 3 do not need to assess this area, but organizations can refer to A.2 Assets: Hardware and Software, A.4 Security/Protection: Virus and Malware Protection, A.6 Security/Protection: Security Configuration, A.7 Updates: Software Updates, and A.8 Backup: Backing up important data covering mobile devices in Cyber Essentials mark.
- B.11.4: Tier 4 Performer need to develop and implement policies and procedures that address the guidelines, requirements, and procedures for using BYOD devices to connect to the organization's network and access the organization's data.
- B.11.5 – B.11.7: The Tier 5 Advocate need to implement cybersecurity measures in organizational BYOD, such as mobile device management (MDM), ensure device compliance and security, and review BYODs that have access to business-critical data at least once a year. In addition, organizations need to have mechanisms in place to prevent the leakage and loss of confidential or sensitive information.

For details about cybersecurity preparedness domains, please refer to Cyber Trust mark. The following is the compliance document/white paper released by HUAWEI CLOUD for tenants.

<HUAWEI CLOUD Security White Paper> A.5.9 Information Assets and Other Related Assets & A.5.10 Acceptable Use of Information and Other Related Assets & A.5.11 Return of Assets

4.1.2 B.8 Asset management

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.8.1 Supporter	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.2 Assets: Hardware and software to ensure that hardware and software present in the environment are identified and protected against common cyber threats.	For details, please refer to section 2.4 (a), (d), (g) - (l) in the Cyber Essentials mark Security Guide "A.2 Assets: Hardware and Software."	
B.8.2 Practitioner	The organization has implemented all the cybersecurity recommendations in the Cyber Essentials mark under A.2 Assets: Hardware and software to ensure that hardware and software present in the environment are identified and protected against common cyber threats.	For details, please refer to section 2.4 (b), (c), (e), (f), and (m) in the Cyber Essentials mark Security Guide "A.2 Assets: Hardware and Software."	
B.8.3 Promoter	The organization has established and implemented policies and procedures on the security requirements, guidelines and detailed steps to classify, handle and dispose of hardware and software assets in the environment securely to ensure that employees have clear direction and guidance.	Customers should establish formal asset management policies and procedures. (including security requirements, processes, guidelines, and detailed procedures) Manage and dispose of assets in the organization by category, for example, define asset owners, specify asset list management and update procedures, define asset inbound and outbound regulations, and specify security storage requirements for software and hardware assets.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.9-A.5.13.
B.8.4 Promot	The organization has established and implemented a process to classify and handle hardware and	Customers should establish risk management methods and procedures that comply with their organizational strategies	● HSS: Asset management

er	software according to their confidentiality and/or sensitivity levels to ensure that they receive adequate security and protection.	to protect assets based on the confidentiality, integrity, and availability of assets. HUAWEI CLOUD **Host Security Service (HSS)** provides a unified management portal for you to query and manage cloud services. It is a security manager for servers and provides asset management (For details, see the product security document on the right.) functions. Manages and analyzes security asset information such as accounts, ports, processes, web directories, and software.	
B.8.5 Promoter	The organization has defined and allocated roles and responsibilities to ensure that it is clear who is responsible to maintain, support and manage the hardware and software assets in the inventory list.	Customers should establish a formal asset management procedure to discover new information assets in time, maintain the latest asset list, and assign owners for the assets to ensure that the owners are clear about who is responsible for maintaining, supporting, and managing the hardware and software assets in the inventory list.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.9-A.5.13.
B.8.6 Performer	The organization has established and implemented asset discovery tools that are appropriate and recognized in the industry to scan and discover assets that are connected to its network to ensure that all the assets can be managed securely.	Customers should establish a formal asset management procedure to discover new information assets in time and maintain the latest asset list. HUAWEI CLOUD **Host Security Service (HSS)** provides a unified management portal for you to query and manage cloud services. It is a security manager for servers and provides asset management functions. Manages and analyzes security asset information such as accounts, ports, processes, web directories, and software.	● HSS： HSS Asset Management HSS Asset Overview
B.8.7 Performer	The organization has established and implemented an acceptable use policy on the rules and restrictions for hardware and software assets to ensure that the assets are being managed appropriately and securely.	Customers should establish formal asset management rules, policies, and procedures to ensure that software and hardware in the cyber security domain are clearly marked and included in the asset management scope.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD

			Compliance with ISO 27001> A.5.9-A.5.13.
B.8.8 Performer	The organization has established and implemented a policy and process to ensure that the hardware and software asset inventory is consistent and updated organization wide.	Customers should establish and maintain a comprehensive inventory of IT assets categorized by business criticality.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.9-A.5.13.
B.8.9 Advocate	The organization has established and implemented the use of an asset inventory management system that is appropriate and recognized in the industry to track and manage hardware and software assets to ensure accuracy and avoid oversight.	Customers should establish a formal asset management procedure based on industry-recognized standards or documents (such as ISO27001 or NIST CSF), discover new information assets in a timely manner, and maintain the latest asset list. HUAWEI CLOUD **Host Security Service (HSS)** provides a unified management portal for you to query and manage cloud services. It is a security manager for servers and provides asset management functions. Manages and analyzes security asset information such as accounts, ports, processes, web directories, and software.	● HSS: HSS Asset Management HSS Asset Overview
B.8.10 Advocate	Asset risks are being addressed as part of the risk assessment framework and reported to the Board and/or senior management to ensure that they are not neglected.	Customers should establish risk management methods and procedures that comply with their organizational strategies based on the confidentiality, integrity, and availability of assets, identify asset risks, and report the risks to the management of the organization.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.9-A.5.13.

4.1.3 B.9 Data protection and privacy

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.9.1 Supporter	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.3 Assets: Data to ensure that business-critical data (including personal data, company secrets, intellectual property, etc.) can be identified, located and secured.	For more information, please refer to Cyber Essentials mark, "A.3 Assets: Data."	
B.9.2 Supporter	The organization has defined and applied a process to report any business-critical data (including personal data, company secrets, intellectual property, etc.) breach and to ensure that stakeholders such as the management, relevant authorities and relevant individuals are kept informed.	Customers should establish and implement a data breach incident management process to monitor and record data breach incidents, prevent the impact of a data breach from expanding, and notify affected parties (such as management, relevant authorities, and relevant individuals) of the data breach in a timely manner. HUAWEI CLOUD provides **Cloud Trace Services (CTS)** to provide customers with operational records of cloud service resources for user query, audit, and backtracking. (For details, see the product security document on the right.) HUAWEI CLOUD **Data Security Center (DSC)** provides customers with basic data security capabilities, such as data classification, data security risk identification, data watermark source tracing, and data anonymization. The data security overview integrates the status of each phase in the data security lifecycle and displays the overall data security situation on the cloud. In addition, HUAWEI CLOUD released the <HUAWEI CLOUD Cyber Security and Privacy Protection FAQ white paper> on its official website, which describes the data breach management process. (For details, see the product	● CTS: Data audit Data protection technology ● FAQ Whitepaper: Section 1.3.11

		security document on the right.) Customers can plan their own data breach management process based on HUAWEI CLOUD security best practices. including event reporting, emergency plan, and recovery process.	
B.9.3 Supporter	The organization that uses cloud service has established and implemented the cloud shared responsibility model with the Cloud Service Provider (CSP) in terms of data privacy and security (e.g., agreement with the CSP to establish clear roles and responsibilities between the organization and the CSP).	For details, please refer to chapter 3 " HUAWEI CLOUD Security Responsibility Sharing Model".	For details, see chapter 3 " HUAWEI CLOUD Security Responsibility Sharing Model".
B.9.4 Practitioner	The organization has implemented all the cybersecurity recommendations in the Cyber Essentials mark under A.3 Assets: Data to ensure that business-critical data (including personal data, company secrets, intellectual property, etc.) can be identified, located and secured.	For details, please refer to Cyber Essentials mark under A.3 Assets: Data.	
B.9.5 Promoter	The organization has established and implemented policies and procedures to carry out risk classification and handle business-critical data (including personal data, company secrets, intellectual property, etc.) according to their confidentiality and/or sensitivity levels to ensure that they receive adequate security and protection.	Customers are responsible for protecting their content data on the cloud. They should take security measures to protect content data such as business-critical data based on the confidentiality and sensitivity levels of the organization. Regarding data isolation, HUAWEI CLOUD recommends that data be distinguished and isolated at the beginning of the data life cycle by first running a classification and risk analysis on the customer's data. Based on the risk analysis results, clarify the storage location, storage services and security measures to protect data. To meet compliance requirements, HUAWEI CLOUD also provides customers with a range of data storage services that follow advanced	< Huawei Cloud Data Security White Paper> 4 Huawei Cloud Data Security Governance System 6.1.1 Data Identification and Classification

		industry standards for data security lifecycle management using excellent technologies, practices, and processes in authentication, rights management, access control, data isolation, transmission security, storage security, data deletion, and physical destruction. It also ensures that tenant privacy, ownership and control over their data are not infringed upon, providing users with the most effective data protection. For more details, please refer to the < Huawei Cloud Data Security White Paper>. HUAWEI CLOUD **Data Security Center (DSC)** provides customers with basic data security capabilities, such as data classification, data security risk identification, data watermark source tracing, and data anonymization. The data security overview integrates the status of each phase in the data security lifecycle and displays the overall data security situation on the cloud.	
B.9.6 Promoter	The organization has established and implemented policies and procedures to document the data flow diagram of business-critical data (including personal data, company secrets, intellectual property, etc.) through information systems and programs in the organization and implement relevant enforcement measures to ensure that they stay within the environment.	See B.9.5 for further details.	
B.9.7 Promoter	The organization has established and implemented policies and procedures to handle business-critical data (including personal data, company secrets, intellectual property, etc.) securely and to protect business-critical data according to their classifications and	See B.9.5 for further details.	

	requirements (e.g., collect, use, protect, dispose).		
B.9.8 Performer	The organization has established and implemented data management policies and procedures through the guidelines, requirements and steps to handle business-critical data (including personal data, company secrets, intellectual property, etc.) at rest, in transit and in use securely.	Customers should release policy documents or guides related to data security to instruct employees in the organization to implement full-lifecycle protection for business-critical data. See B.9.5 for further details.	< Huawei Cloud Data Security White Paper> 5.1 Static Data Security 5.2 Dynamic Data Security 5.3 Security in Data Processing 6.4 Data Transmission
B.9.9 Performer	The organization has defined and allocated roles and responsibilities to ensure that it is clear who is responsible to maintain, support and manage the data assets in the inventory list.	See B.9.5 for further details.	
B.9.10 Performer	The organization using encryption has defined and applied a process on the use of recommended protocol and algorithm and minimum key length to ensure that it is secure and not obsolete.	Customers is responsible for defining and using secure transmission protocols and encryption algorithms, specifying the minimum key length, and ensuring that data encryption measures are updated periodically.	< Huawei Cloud Data Security White Paper> 5.1.3 Storage Encryption 5.2.1 Encrypted Transmission
B.9.11 Advocate	The organization uses encryption to protect its data and has established and implemented cryptographic policies and processes to ensure that the keys are being handled securely throughout the cryptography key management lifecycle.	Customers are responsible for protecting their content data in the cloud. The customer shall implement security control measures for ICT systems, including vulnerability and patch management, network security configuration, network segmentation, data leak prevention, network traffic encryption, endpoint protection, software, hardware, and data integrity verification, and data encryption. HUAWEI CLOUD provides the **Data Encryption Workshop (DEW)** for customers. The DEW key management function enables you to centrally manage keys	● DEW: Viewing Dedicated HSM Instances Key Management

		throughout the lifecycle. Without authorization, no one except the customer cannot obtain a key to decrypt data, ensuring data security on the cloud. The DEW uses a hierarchical key management mechanism to facilitate key rotation at each layer. (For details, see the product security document on the right.) HUAWEI CLOUD uses the hardware security module (HSM) to create and manage keys for customers. HSM has FIPS140-2 (level 2 and level 3) mainstream international security certification, helping users meet data compliance requirements and prevent intrusion and tampering. Even HUAWEI CLOUD O&M personnel cannot steal customer root keys. DEW allows customers to import their own keys as CMKs for unified management, facilitating seamless integration and interconnection with customers' existing services. (For details, see the product security document on the right.) HUAWEI CLOUD **Data Security Center (DSC)** provides customers with basic data security capabilities, such as data classification, data security risk identification, data watermark source tracing, and data anonymization. The data security overview integrates the status of each phase in the data security lifecycle and displays the overall data security situation on the cloud.	
B.9.12 Advocate	The organization has established and implemented policies and procedures allowing only authorized devices with secure protocols to communicate, store and transfer business-critical data (including personal data, company secrets, intellectual property, etc.) in the organization.	Customers can use **Cloud Certificate Manager (CCM)** to establish secure HTTPS connections for their websites or web services. At the same time, **SSL Certificate Manager (SCM)** of HUAWEI CLOUD provides customers with one-stop certificate lifecycle management, implementing trusted identity authentication and secure data transmission for websites. The platform cooperates with world-renowned digital certificate authority to provide users with the SSL certificate purchase function. Customers can also upload local external SSL certificates to the IoT platform to centrally manage internal and external SSL certificates. (For details, see the product security document on the	● CCM Service: Enabling HTTPS Encryption for Websites Deploying SSL Certificates to the Cloud in One Click Best Practices for Private Certificate Management

		right.) After deploying the service, customers can replace the HTTP protocol used by the service with the HTTPS protocol to eliminate security risks of the HTTP protocol. (For details, see the product security document on the right.) This service can be used for website authentication, application authentication, and data transmission protection. SSL certificates can be used in SLB, CDN, WAF, Anti-DDoS, and ECS.	
B.9.13 Advocate	The organization has established and implemented policies and procedures to report on data protection and privacy risks and initiatives to the Board and/or senior management to ensure that they are kept informed.	Customers shall regularly conduct Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (PIA) on business-critical data, evaluate the risks of data in the enterprise and the effectiveness of protection measures, and report to the board of directors or management team of the organization.	<HUAWEI CLOUD Privacy Protection White Paper> 4.2 Huawei Cloud Privacy Protection System

4.1.4 B.10 Backups

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.10.1 Supporter	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.8 Backup: Back up essential data to ensure that the organization's essential data is backed up and stored securely.	For more information, please refer to the cybersecurity measures in "A.8 Backup: Backing Up Basic Data" A.8.4(a), (b), (e), (g), (h), (j) in Cyber Essentials mark.	
B.10.2 Practitioner	The organization has implemented all the cybersecurity recommendations in the Cyber Essentials mark under A.8 Backup: Back up essential data to ensure that	For more information, please refer to the cybersecurity measures in "A.8 Backup: Backing Up Basic Data" A.8.4 (c), (d), (f), (i), and (k) in Cyber Essentials mark.	

	the organization's essential data is backed up and stored securely.		
B.10.3 Practitioner	The organization has established and implemented automated backup processes to ensure that the backup tasks are carried out without fail and without the need for human intervention.	Customers can use **Cloud Backup and Recovery (CBR)** to back up cloud servers, disks, file services, off-cloud and VMware virtual environments. Through the policy interface, customers can set a backup policy and bind the policy to a vault to implement automatic backup. (For details, see the product security document on the right.)	● CBR Service: Using a Custom Script to Implement Application-Consistent Backup CBR Application Case1: Creating an ECS Backup CBR Application Case2: Implementing Automatic Backup for a Vault
B.10.4 Promoter	The organization has established and implemented backup plan(s) on the types, frequency and storage of backups to ensure that there is clarity of the steps to be taken to backup business-critical data in the organization.		
B.10.5 Promoter	The organization has established and implemented the use of technology solutions for data backup and recovery, and the solutions implemented are appropriate and recognized in the industry to ensure that it can carry out reliable data backup and restoration.	Customers can use the snapshot function of **Elastic Volume Service (EVS)** to restore data to the snapshot point in time when data is lost. (For details, see the product security document on the right.) HUAWEI CLOUD also provides **Image Management Service (IMS)** customers can use to back up cloud server instances and use the backup images to restore cloud server instances when the software environment of the instances is faulty. (For details, see the product security document on the right.)	● EVS: EVS Snapshot (OBT) Redundant Array of Independent Disks (RAID) ● IMS: ECS Backup and Recovery IMS Practices Overview
B.10.6 Performer	The organization has established and implemented backup and recovery policies and procedures on the requirements, guidelines and detailed steps to ensure that there is a consistent guidance and direction for performing backup and recovery in the organization.	Customer is responsible for developing and implementing procedures and policies for backup and recovery. See sections B.10.3 - B.10.5 for further details	See sections B.10.3 - B.10.5 for further details

B.10.7 Performer	The organization has defined and allocated roles and responsibilities to ensure that it is clear who is responsible and accountable to perform and manage backup from creation to destruction.	Customers shall identify and assign personnel to perform and manage backups for content data or business critical data on the Enterprise Cloud.	This is the responsibility of tenants.
B.10.8 Advocate	The organization has established and implemented a backup control sheet for the backup data storage media with the purpose of including backup, time of backup, data encryption, retention date and the employee(s) assigned the task of backup to ensure that all the key information are documented.	HUAWEI CLOUD provides multi-granularity data backup and archiving services to meet customers' requirements in different scenarios. Customers can use the version control function of **Object Storage Service (OBS)** and the following functions of Cloud Backup Service (CBR): 1) **Volume Backup Service (VBS)** and 2) **Cloud Server Backup Service (CSBS)** records and manages multi-granularity backup storage media information. (For details, see the product security document on the right.)	● OBS: Configuring Versioning ● VBS: VBS Backup Management ● CSBS: Creating a User and Granting CSBS Permissions Creating a Backup Policy
B.10.9 Advocate	The organization has established and implemented policies and procedures to report backup related matters to the cybersecurity committees/forums to ensure that senior management is kept informed.	Customers should have policies and procedures in place to define the requirements for regular reporting to the organization's management on backup related matters.	This is the responsibility of tenants.
B.10.10 Advocate	The organization has established and implemented policies and procedures to perform reviews on the backup status regularly to ensure that failed backup jobs are addressed and remediated.	Customers are responsible for testing backups at least semi-annually or more frequently. Customers can use the **Cloud Backup and Recovery (CBR)** service provided by HUAWEI CLOUD to protect **Elastic Volume Service (EVS)** disks, **Elastic Cloud Servers (ECSs)**, and **Bare Metal Servers (BMS)**. Cloud backup supports snapshot-based backup services and uses backup data to restore data on servers and EVS disks. In	● CBR: Periodic Recovery Drills Using the Backup Data

		addition, users can synchronize backup data from the offline backup software BCManager and verify the integrity of the backup data. (For details, see the product security document on the right.)	

4.1.5 B.12 System security

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.12.1 Supporter	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.6 Secure/Protect: Secure configuration and A.7 Update: Software updates to ensure that the hardware and software uses secure and updated settings.	For more information, please refer to Cyber Essentials mark: - A.6 Security/protection: security configuration A.6.4 (a) - (e); -A.7 Update: Software update A.7.4 (a) and (b).	
B.12.2 Practitioner	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.6 Secure/Protect: Secure configuration and A.7 Update: Software updates to ensure that the hardware and software uses secure and updated settings.	For more information, please refer to Cyber Essentials mark: - A.6 Security/protection: security configuration A.6.4 (f) - (h); -A.7 Update: Software update A.7.4 (c) and (d).	
B.12.3 Practitioner	The organization has performed monitoring on updates and patches installed to ensure that any impact or adverse effects can be identified and rectified in a timely manner.	Customers need to take measures to monitor the installed updates and patches of the systems or applications in the organization so that any outdated or vulnerable updates and patches can be identified in a timely manner. The customer is responsible for the security configuration and management tasks (including updates and security patches) necessary to deploy cloud services such as virtual	● COC: Patch Management One-Stop Resource O&M

		networks, virtual hosts, and guest virtual machines and containers. Customers can use the **Cloud Operations Center (COC)** of HUAWEI CLOUD to perform centralized O&M on HUAWEI CLOUD services. (including fault management, patch management, batch O&M, and chaos drills) COC patch management allows users to manage patches on ECSs or CCE instances. (For details, see the product security document on the right.) With the patch management capability, users can implement OS patch compliance scanning and OS patch compliance recovery. (For details, see the product security document on the right.)	
B.12.4 Promoter	The organization has defined and applied a process to ensure secure configurations are applied across all systems, servers, operating systems and network devices.	Customers must formulate security configuration baselines for all systems and periodically check the baselines. If the security configuration baseline is not met, assess the risks and develop compensation measures. Customers can check host baselines through HUAWEI CLOUD **Host Security Service (HSS)**. It can check system password complexity policies, typical weak passwords, risky accounts, and common system and middleware configurations to identify insecure items and prevent security risks. (For details, see the product security document on the right.)	● HSS: HSS Configuring Policies HSS Multi-Cloud Management and Deployment
B.12.5 Promoter	The organization has defined and applied a log management process to store and classify the different types of logs securely to ensure that they can be used to troubleshoot effectively.	Customers are responsible for specifying and defining the log management process. **Log Tank Service (LTS)** provided by HUAWEI CLOUD collects, queries, and stores logs in real time. Its records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing. (For details, see the product security document on the right.)	Log Tank Service: ● Using Scripts to Invoke LTS APIs for Custom Operations ● Analyzing Huawei Cloud WAF Logs for O&M Insights ● Analyzing Huawei Cloud ELB Access

			Logs for O&M Insights
B.12.6 Promoter	The organization has defined and applied a patch management process to test and install the updates and patches securely to ensure that there are no adverse effects.	Customers can use the **Cloud Operations Center (COC)** of HUAWEI CLOUD to perform centralized O&M on HUAWEI CLOUD services. (including fault management, patch management, batch O&M, and chaos drills) COC patch management allows users to manage patches on ECSs or CCE instances. (For details, see the product security document on the right.) With the patch management capability, users can implement OS patch compliance scanning and OS patch compliance recovery.	● COC: Patch Management One-Stop Resource O&M
B.12.7 Performer	The organization has defined and allocated the roles and responsibilities to oversee, manage and monitor the organization's system security (i.e., secure configuration, logging, update and patching) to ensure that employees are clear on the tasks assigned to them.	Customers should be responsible for assigning and assigning oversight, management and monitoring of the Organization's system security. (i.e., security configuration, logging, updating, and patching) roles and responsibilities to ensure that employees clearly understand the tasks assigned to them, such as appropriate awareness training or online courses for employees on configuration, logging and updating of system security.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 8.2 Secure Design, 8.3 Secure Coding and Testing, and 8.5 Configuration and Change Management.
B.12.8 Performer	The organization has established and implemented policies and procedures on the security configuration requirements, guidelines and detailed steps to ensure that they are aligned with the security standards.	Customers should formulate security configuration baselines for all systems and periodically check the baselines. If the security configuration baseline is not met, assess the risks and develop compensation measures. Customers can check host baselines through HUAWEI CLOUD **Host Security Service (HSS)**. It can check system password complexity policies, typical weak passwords, risky accounts, and common system and middleware configurations to identify insecure items and prevent security risks. (For details, see the product security document on the right.)	● HSS: HSS Configuring Policies HSS Multi-Cloud Management and Deployment

B.12.9 Performer	The organization has established and implemented a secure logging policy and procedure with the requirements, guidelines and detailed steps to store, retain and delete the logs from unauthorized access.	**Log Tank Service (LTS)** provided by HUAWEI CLOUD collects, queries, and stores logs in real time. Its records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing. In addition, HUAWEI CLOUD has a centralized and complete log big data analysis system. (For details, see the product security document on the right.) The system collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components to support cyber security event backtracking and compliance. (For details, see the product security document on the right.)	● LTS: LTS Permissions Management LTS Log Management
B.12.10 Performer	The organization has established and implemented policies and procedures with the requirements, guidelines and detailed steps to perform and install patches/updates to ensure that the system(s) is/are patched or updated within the defined timeframes according to their priority.	Customers can use the **Cloud Operations Center (COC)** of HUAWEI CLOUD to perform centralized O&M on HUAWEI CLOUD services. (including fault management, patch management, batch O&M, and chaos drills) COC patch management allows users to manage patches on ECSs or CCE instances. (For details, see the product security document on the right.) With the patch management capability, users can implement OS patch compliance scanning and OS patch compliance recovery.	● COC: Patch Management ● One-Stop Resource O&M
B.12.11 Advocate	The organization has implemented a configuration management tool/solution that is appropriate and recognized in the industry to ensure that the system's configurations are maintained in a desired and consistent state.	Customers can use the **SecMaster service** of HUAWEI CLOUD. SecMaster is a next-generation cloud native security operation platform. Based on years of cloud security experience of HUAWEI CLOUD, it enables integrated and automatic security operations through cloud asset management, security posture management, security information and incident management, security orchestration and automatic response. (For details, see the product security document on the right.) Customers can have a bird's-eye view of the entire cloud security, simplify cloud security configuration, and set and maintain cloud protection policies to prevent risks in advance. (For details, see the product security document on the right.) It makes threat detection and response smarter and faster, helping	● SecMaster: Operation Guide to Data Transfer Security Orchestration Configuring Policies

		customers achieve integrated and automated security operations management.	
B.12.12 Advocate	The organization has established and implemented policies and procedures to ensure that the system's configuration requirements are aligned with the industry benchmarks and standards, e.g., CIS configuration benchmarks.	Customers can use HUAWEI CLOUD **Configuration Audit Service (Config)** to manage configurations of cloud services. HUAWEI CLOUD Config provides users with global resource configuration search, historical configuration tracing, and continuous audit and evaluation capabilities based on resource configurations to ensure that resource configuration changes on the cloud meet customer expectations. (For details, see the product security document on the right.)	● Config: Adding a Predefined Rule Viewing Noncompliant Resources Managing Conformance Packages
B.12.13 Advocate	The organization has established and implemented policies and procedures to ensure that the systems' configurations are being complied and the risks as a result of non-compliance are being addressed.	Customers should responsible for establishing policies and procedures for compliance with the system configuration.	This is the responsibility of tenants.

4.1.6 B.13 Anti-virus/anti-malware

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.13.1 Supporter	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.4 Secure/Protect: Virus and malware protection to ensure that there is security protection against malicious software such as virus.	For more information, please refer to the cybersecurity measures A4.4 (a) to (d), (f), and (j) to (l) in Cyber Essentials mark "A.4 Security/Protection: Virus and Malware Protection"	
B.13.2 Practiti	The organization has implemented all the cybersecurity recommendations in the Cyber	For more information, please refer to the cybersecurity measures A4.4 (e), (g) to (i) in Cyber Essentials mark "A.4 Security/Protection: Virus and Malware Protection"	

oner	Essentials mark under A.4 Secure/Protect: Virus and malware protection to ensure that there is security protection against malicious software such as virus.		
B.13.3 Practitioner	The organization has established and implemented the use of anti-virus and/or anti-malware solution(s) that is/are appropriate and recognized in the industry with features such as real-time malware detection and email protection, to ensure that it/they can protect the organization adequately.	Customers should have safeguards in place to protect against malicious attacks or intrusions, including intrusion prevention and detection, anti-virus and malware protection. Customers can use **Host Security Service (HSS)** of HUAWEI CLOUD. HSS provides intrusion detection and malicious program isolation and removal functions to help customers detect security threats in servers, virtual environments, and hosts/containers in a timely manner and implement in-depth detection and removal. At the same time, HUAWEI CLOUD can also provide an **Anti-DDoS service**, **Web Application Firewall (WAF)** to help users accurately and effectively implement comprehensive protection against traffic-based attacks and application level and data-level attacks. (For details, see the product security document on the right.)	● HSS: Best Practices for Defense Against Ransomware ● AAD: Anti-DDoS Best Practices ● WAF: Best Practices for One-Click Deployment
B.13.4 Practitioner	The organization has established and implemented web filtering to protect the business from surfing malicious sites.	HUAWEI CLOUD deploys the DoS/DDoS cleaning layer, next-generation firewall, intrusion prevention system layer, and website application firewall layer at the network border to filter the network and protect enterprise resources on HUAWEI CLOUD from malicious websites. At the same time, HUAWEI CLOUD can also provide an **Anti-DDoS service**, **Web Application Firewall (WAF)** to help users accurately and effectively implement comprehensive protection against traffic-based attacks and application level and data-level attacks. (For details, see the product security document on the right.)	● AAD: Anti-DDoS Best Practices ● WAF: Best Practices for One-Click Deployment
B.13.5 Practitioner	The organization has defined and applied the process to isolate and contain the virus and/or malware upon confirmation of attack to	Customers should establish an incident and problem management process to identify, record, and classify incidents based on priority, perform consistent and integrated monitoring, handling, and follow-up on	This is the responsibility of tenants. For details about the security

	ensure minimal spread and damage caused.	operational and security incidents, ensure that root causes are identified and eliminated to prevent repeated incidents, establish incident response procedures for different scenarios, and develop communication plans. Minimize the impact of adverse events and enable timely recovery.	practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper>.
B.13.6 Promoter	The organization has defined and applied the process to run codes or applications of unknown origin within an isolated testing environment to test for the presence of virus and/or malware prior to their use in the working environment.	Customers should establish a formal environment isolation mechanism to logically isolate the development environment, test environment, and production environment, improve the self-protection and fault tolerance capabilities against external intrusions and internal violations, and reduce the risks of unauthorized access to or changes to the running environment.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper>.
B.13.7 Performer	The organization has defined and allocated the roles and responsibilities for employees to oversee, manage and maintain the anti-virus and/or anti-malware solution(s) to ensure clarity for the relevant employees of their required tasks.	Customers should define and assign the roles and responsibilities of employees in terms of antivirus or anti-malware software through policy or process documents, and carry out corresponding publicity or awareness training. For details about antivirus and anti-malware capability building and solution design, see the HSS product documentation.	● HSS: Best Practices for Defense Against Ransomware
B.13.8 Advocate	The organization has established and implemented policies and processes to subscribe to threat intelligence with external parties and to share and verify information relating to cyberattacks which includes virus and/or malware attacks.	Customers should ensure that they have effective crisis communication measures in place to inform internal and external stakeholders and regulators in a timely manner.	This is the responsibility of tenants.
B.13.9 Advocate	The organization has established and implemented policies and processes to review and report findings on virus and/or malware to the Board and/or senior	Customers should develop and implement policies and procedures for virus or malware audits and debrief audit findings with the organization's board of directors or management.	This is the responsibility of tenants. For details about the security practices of HUAWEI

	management to ensure that they are kept informed.		CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.8.7.
B.13.10 Advocate	The organization has established and implemented scanning and detection on indicators of compromise to ensure that anomalies and suspicious activities can be identified early.	Customers should monitor and detect viruses or malware and conduct regular security testing, preferably using predictive indicators.	

4.1.7 B.14 Secure Software Development Lifecycle (SDLC)

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.14.5 Advocate	The organization has established and implemented a SDLC framework with cybersecurity measures and requirements to manage the software development life cycle to ensure that areas such as data integrity, authentication, authorization, accountability and exception handling can be addressed.	Customer should formulate project management methods and security development management regulations, implement security management measures for system security acquisition and development, and strictly isolate access to each environment.	This is the responsibility of tenants.
B.14.6 Advocate	The organization has established and implemented security guidelines and requirements in its system and/or application development, e.g., secure coding to ensure that it adheres to the security principles.	Customers should ensure that their application development processes follow a secure system development life cycle approach, implementing security standards throughout the application security development life cycle. HUAWEI CLOUD provides **CodeArts**, a one-stop secure and trusted DevSecOps platform (For details, see the product security document on the right.) for software development, to provide customers with one-stop software development services throughout the lifecycle.	● One-stop DevSecOps of CodeArts: Req Management Repo Pipeline Build Deploy

			Artifact Code Check TestPlan
B.14.7 Advocate	The organization has established and implemented the change management policy and process to ensure that changes or deployment to the production environment is reviewed and tested securely with a rollback plan in place to ensure that the change is controlled.	The customer should establish a formal change management procedure to identify, classify, and prioritize changes based on the importance of information assets. Identified changes should be tested, assessed for cybersecurity risk, and authorized and approved before they are made. The customer should consider the emergency change process in the change management requirements and implement the change rollback and rollback procedures. HUAWEI CLOUD provides **Cloud Trace Services (CTS)** to provide customers with operational records of cloud service resources for user query, audit, and backtracking. All personnel operations can be recorded in real time and systematically so that customers can perform post-audit on each change. (For details, see the product security document on the right.)	● CTS: Data audit Data protection technology
B.14.8 Advocate	The organization has established and implemented a policy and process to perform security testing on the system and/or application before deployment to ensure that the security weaknesses and vulnerabilities are identified.	Customers should ensure that their application development processes follow a secure system development life cycle approach, implementing security standards throughout the application security development life cycle. HUAWEI CLOUD provides **CodeArts**, a one-stop secure and trusted DevSecOps platform for software development, to provide customers with one-stop software development services throughout the lifecycle. (For details, see the product security document on the right.)	● One-stop DevSecOps of CodeArts: Req Management Repo Pipeline Build Deploy Artifact Code CheckTestPlan

4.1.8 B.15 Access control

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.15.1 Supporter	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.5 Secure/Protect: Access control to ensure that there are cybersecurity measures in place over who has access to the data and assets.	For more information, please refer to the cybersecurity measures in A5.4 (a) - (i) in Cyber Essentials mark "A.5 Security/ Protection: Access Control" in Chapter 5.1.	
B.15.2 Practitioner	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.5 Secure/Protect: Access control to ensure that there are cybersecurity measures in place over who has access to the data and assets.	For more information, please refer to the cybersecurity measures in A5.4 (j) - (p) in Cyber Essentials mark "A.5 Security/ Protection: Access Control" in Chapter 5.1.	
B.15.3 Practitioner	The organization performs regular role matrix review at least on an annual basis on the systems to ensure that the roles commensurate with the activities the employee, contractor and/or third party is allowed to perform.	Customers shall regularly review the account permission scope to ensure that user permission application, change, or withdrawal can be managed in a timely manner based on the identity and access control policy. Customers can use **Identity and Access Management (IAM)** to view the list of IAM users (sub-users who access HUAWEI CLOUD) and their IAM groups, access key pairs, and last login dates. The IAM service is used to check the roles and permissions of the personnel corresponding to the account. (For details, see the product security document on the right.)	● IAM: Creating a User Group and Assigning Permissions Permissions Management
B.15.4 Promoter	The organization has defined and applied a process to approve and follow up on account access and role matrix review to ensure that	Account access should be approved by the customer and the ACLs for the role matrix should be reviewed.	● IAM: Permissions Management

	unauthorized entry has been rectified and signed off.	HUAWEI CLOUD **Identity and Access Management (IAM)** Service supports user group-based permission management, allows users to set password policies, password change periods. (For details, see the product security document on the right.) HUAWEI CLOUD IAM supports user group-based permission management, allows users to set login policies, account locking policies, account disabling policies, and session timeout policies that meet customers' status, and provides IP-based ACLs. (For details, see the product security document on the right.)	Assigning Dependency Roles
B.15.5 Promoter	The organization has defined and applied a process to ensure that employees are assigned roles based on principle of least privilege and segregation of duties.	Customers shall implement role-based access control and permission management, comply with the minimum principle of knowledge and use on demand, and ensure that there is no conflict of interest between responsibilities. Ensure that access to information technology systems can be traced back to individuals.	For details about HUAWEI CLOUD security practices, see B.15.3.
B.15.6 Promoter	The organization has established and implemented a secure logon policy and procedure on the requirements, guidelines and detailed steps of gaining access to sensitive and/or business-critical data as well as privileged access to ensure that the access is controlled and restricted.	Customers should develop a privileged account management mechanism to control and restrict the allocation and use of privileged access rights. Strict login/use approval requirements and processes should be set for administrator accounts or super administrator accounts. Administrator accounts can be logged in only after being approved by the senior management of the organization.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper>.
B.15.7 Performer	The organization has established and implemented a passphrase policy and procedure on the requirements, guidelines and detailed steps on setting and updating passphrases to provide guidance and direction on what constitutes strong passphrases.	Account access should be approved by the customer and the ACLs for the role matrix should be reviewed. HUAWEI CLOUD **Identity and Access Management (IAM)** Service supports user group-based permission management, allows users to set password policies, password change periods. (For details, see the product security document on the right.) HUAWEI CLOUD IAM supports user group-based permission management, allows users to set login policies,	● IAM: Permissions Management Assigning Dependency Roles

		account locking policies, account disabling policies, and session timeout policies that meet customers' status, and provides IP-based ACLs. (For details, see the product security document on the right.)	
B.15.8 Performer	The organization has established and implemented a user access control policy and procedure on the requirements, guidelines and detailed steps to restrict and authorize users' access to the organization's assets.	Customers shall implement role-based access control and permission management, comply with the minimum principle of knowledge and use on demand, and ensure that there is no conflict of interest between responsibilities. HUAWEI CLOUD provides **Identity and Access Management (IAM)** for customers to manage their accounts that use cloud resources. Customers can use IAM to perform role-based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system (For details, see the product security document on the right.), for example, setting an access control list (ACL), to prevent malicious access from untrusted networks. Customers should establish a user access management mechanism to restrict and supervise the access to the system based on the least privilege principle. (For details, see the product security document on the right.)	● IAM: Cross-Region Permissions Assignment Creating a Custom Policy
B.15.9 Performer	The organization has established and implemented secure remote access policies and procedures on the requirements, guidelines and detailed steps to protect the information being accessed remotely.	The Customer shall be responsible for the development and implementation of policies and procedures for remote access. HUAWEI CLOUD provides encrypted transmission methods, such as **Virtual Private Network (VPN)** and HTTPS, for customers to establish secure remote access. (For details, see the product security document on the right.)	● VPN: Using VPN to Encrypt Data over Direct Connect Lines VPN Security Overview
B.15.10 Advocate	The organization has established and implemented policies and processes to review any sign of access compromise and to report the result to the Board and/or senior	In particular, customers should have procedures in place to record and monitor any unauthorized access activity. Customers can also use the **Cloud Trace Service (CTS)** to provide tenants with records of operations on cloud service	● CTS CTS Best Practices

	management to ensure that they are kept informed.	resources for query, audit, and backtracking. (For details, see the product security document on the right.)	
B.15.11 Advocate	The organization has established and implemented a privileged access solution that is appropriate and recognized in the industry to authenticate users and authorize access based on their roles to ensure that there is a more efficient and effective way of managing access.	Customers shall implement role-based access control and permission management, comply with the minimum principle of knowledge and use on demand, and ensure that there is no conflict of interest between responsibilities. HUAWEI CLOUD provides **Identity and Access Management (IAM)** for customers to manage their accounts that use cloud resources. Customers can use IAM to perform role-based fine-grained permission control. The administrator can assign permissions for cloud resources to users based on their responsibilities and set security policies for users to access the cloud service system (For details, see the product security document on the right.), for example, setting an access control list (ACL), to prevent malicious access from untrusted networks. Customers should establish a user access management mechanism to restrict and supervise the access to the system based on the least privilege principle. (For details, see the product security document on the right.)	● IAM: Cross-Region Permissions Assignment Creating a Custom Policy

4.1.9 B.16 Cyber threat management

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.16.4 Performer	The organization has established and implemented a log monitoring policy, process and procedure on the requirements, guidelines and detailed steps to perform monitoring of security logs for threats and abnormality.	Customers should establish logging and monitoring procedures for critical ICT operations. **Cloud Trace Service (CTS)** records changes made by operators to resources and system configurations on HUAWEI CLOUD. You can query, audit, and backtrack the records. (For details, see the product security document on the right.)	● CTS: CTS Best Practices CTS Configuring Key Event Notifications

B.16.5 Performer	The organization has defined and allocated the roles and responsibilities to carry out log monitoring and review on its systems, investigating the incidents and reporting to relevant stakeholders.	Customers should develop effective crisis communication measures, define and assign roles and responsibilities for log monitoring, incident investigation and incident reporting, so that all relevant internal and external stakeholders are informed in a timely manner.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper>.
B.16.6 Performer	The organization has implemented Security Information and Event Management (SIEM) to store the logs centrally for correlation and to ensure that the logs are monitored more effectively.	Customers should establish logging and monitoring procedures for critical ICT operations. **Log Tank Service (LTS)** provided by HUAWEI CLOUD collects, queries, and stores logs in real time. Its records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing. Combining with **CLOUD Eye Service (CES)**, Customers can monitor user login logs in real time. When malicious logins occur, an alarm is generated and requests from the IP address are rejected. (For details, see the product security document on the right.)	● LTS: Log Management Querying Real-Time Traces Multi-Account Log Center ● CES: Best Practices of Event Monitoring Cloud Service Monitoring
B.16.7 Performer	The organization has established and implemented a security baseline profile on its systems to analyze and perform monitoring to ensure that anomalies are identified.	Customers shall establish and implement continuous monitoring measures to identify security risks such as security threats and vulnerabilities and corresponding technical developments. Customers can use the **SecMaster service** of HUAWEI CLOUD. SecMaster is a next-generation cloud native security operation platform. Based on years of cloud security experience of Huawei Cloud, it enables integrated and automatic security operations through cloud asset management, security posture management, security information and incident management, security orchestration and automatic response. (For details, see the product security document on the right.) Customers can have a bird's-eye view of the entire cloud security, simplify	● SecMaster: Operation Guide to Data Transfer Security Orchestration Configuring Policies

		cloud security configuration, and set and maintain cloud protection policies to prevent risks in advance. (For details, see the product security document on the right.) It makes threat detection and response smarter and faster, helping customers achieve integrated and automated security operations management.	
B.16.8 Performer	The organization has established and implemented policies and procedures on the requirements, guidelines and detailed steps to carry out in response upon detection of abnormal or suspicious logs to ensure that they are investigated, reported and remediated in a timely manner.	Customers should establish a complete event management process, classify and prioritize events based on appropriate standards and thresholds, and set event warnings for timely response.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper>.
B.16.9 Advocate	The organization has established and implemented advanced analytics processes and solutions that are appropriate and recognized in the industry to detect against abnormal systems and user behavior, e.g., user behavior analytics.	Customers should develop and implement network security monitoring policies and procedures to detect and report anomalous behavior such as physical or logical intrusions, internal and external threats. Customer can detect asset content compliance, scan the configuration to compare it against the baseline, detect weak passwords, and perform other such functions through HUAWEI CLOUD CodeArts Inspector. HUAWEI **CLOUD Eye Service (CES)** provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take corresponding measures. (For details, see the product security document on the right.) HUAWEI CLOUD provides customers with the security management and situation analysis platform of **SecMaster service**, which provides customers with workspace management, security governance, security situation, asset management, risk prevention, threat operation, security orchestration, data collection, and data integration functions.	● CES: Best Practices of Event Monitoring Cloud Service Monitoring ● AAD: Anti-DDoS Best Practices ● WAF: Best Practices for One-Click Deployment ● CTS: CTS Best Practices CTS Configuring Key Event Notifications ● SecMaster:

		SecMaster can be associated with Advanced Anti-DDoS, Host Security Service (HSS), Web Application Firewall (WAF), and Database Security Service (DBSS). Detects various cloud security risks, including DDoS attacks, brute force cracking, web attacks, Trojan horses, zombie hosts, abnormal behavior, vulnerability attacks, and command and control (C&C) attacks. (For details, see the product security document on the right.) In addition, the SecMaster accesses the IAM, DNS, CTS, OBS, and VPC logs generated by users' operations on HUAWEI CLOUD in the target region. Continuously checks whether the IP addresses or domain names of visitors in logs have potential malicious activities and unauthorized behaviors. If an exception is detected, an alarm is generated in a timely manner. (For details, see the product security document on the right.) In addition, various security response scripts are provided to help users automatically analyze and handle alarms and automatically harden the security defense line and security configuration. At the same time, HUAWEI CLOUD can also provide an **Advance Anti-DDoS service (AAD)**, **Web Application Firewall (WAF)**, **Database Security Service (DBSS)**, and **Cloud Trace Services (CTS)** to help users accurately and effectively implement comprehensive protection against traffic-based attacks and application level and data-level attacks, as well as reviewing and auditing incidents. (For details, see the product security document on the right.)	Data Access with a Custom Parser Managing Threat Intelligence Types Threat Situation Screen
B.16.10 Advocate	The organization has established and implemented reporting requirements and dashboards to report detected cybersecurity incidents or anomalies based on their severity to the Board and/or senior management.	Customers can use the consoles of **CLOUD Eye Service (CES)** and **Cloud Trace Service (CTS)** on HUAWEI CLOUD to generate monitoring and handling reports of network security events and report the reports to the organization management.	● CES: Best Practices of Event Monitoring Cloud Service Monitoring ● CTS: CTS Best Practices

			CTS Configuring Key Event Notifications
B.16.11 Advocate	The organization has established and implemented measures and processes to proactively search for threats that are hidden in its IT environment.	Customers should periodically review the security of the information technology system, such as vulnerability scanning and penetration testing, to assess the security of the CSP's environment and manage risks. Customers should establish cyber security organizations and processes and implement continuous monitoring measures to identify security risks such as security threats and vulnerabilities and corresponding technical developments. HUAWEI CLOUD provides customers with the security management and situation analysis platform of **SecMaster service**, which provides customers with workspace management, security governance, security situation, asset management, risk prevention, threat operation, security orchestration, data collection, and data integration functions. SecMaster can be associated with Advanced Anti-DDoS, Host Security Service (HSS), Web Application Firewall (WAF), and Database Security Service (DBSS). Detects various cloud security risks, including DDoS attacks, brute force cracking, web attacks, Trojan horses, zombie hosts, abnormal behavior, vulnerability attacks, and command and control (C&C) attacks. In addition, the SecMaster accesses the IAM, DNS, CTS, OBS, and VPC logs generated by users' operations on HUAWEI CLOUD in the target region. Continuously checks whether the IP addresses or domain names of visitors in logs have potential malicious activities and unauthorized behaviors. (For details, see the product security document on the right.) If an exception is detected, an alarm is generated in a timely manner. In addition, various security response scripts are provided to help users automatically analyze and handle alarms and automatically harden the security defense line and security configuration. In addition, HUAWEI CLOUD provides **Host Security Service (HSS)** to provide host security check and security hardening functions for users. It uses technologies such as	● SecMaster: Data Access with a Custom Parser Managing Threat Intelligence Types Threat Situation Screen ● HSS: HSS Configuring Policies HSS Multi-Cloud Management and Deployment

		log analysis and vulnerability scanning to identify threats, scan vulnerabilities, and harden baseline configurations for hosts (For details, see the product security document on the right.), host servers, and middleware, proactively searches for hidden threats, and provides corresponding rectification solutions. Fix related vulnerabilities and harden patch components with the customer's permission. (For details, see the product security document on the right.)	

4.1.10 B.17 Third-party risk and oversight

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.17.1 Supporter	Domain is not assessable for this tier. However, the organization should ensure that section A.5.4 (b), (g) and (h) in the Cyber Essentials mark under A.5 Secure/Protect: Access control domain on third parties have been implemented. They should also consider the section on securing your access and environment in CSA's cybersecurity toolkit for SME owners and/or educating your employees on security and securing your access and environment in CSA's cybersecurity toolkit for organization leaders and/or IT teams.	This layer does not need to be assessed for Supporter, but the organization should ensure that appropriate measures are in place for the assessment and monitoring of third-party risks, as detailed in Cyber Essentials mark Section A.5.4 (b), (g) and (h) under "A.5 Security/Protection: Access control domain on third parties"	
B.17.2 Practitioner	Domain is not assessable for this tier. However, the organization should ensure that section A.5.4 (b), (g) and (h) in the Cyber Essentials	This layer does not need to be assessed for Practitioner, but the organization should ensure that appropriate measures are in place for the assessment and monitoring of third-party risks, as detailed in Cyber Essentials mark Section A.5.4 (b),	

	mark under A.5 Secure/Protect: Access control domain on third parties have been implemented. They should also consider the section on securing your access and environment in CSA's cybersecurity toolkit for SME owners and/or educating your employees on security and securing your access and environment in CSA's cybersecurity toolkit for organization leaders and/or IT teams.	(g) and (h) under "A.5 Security/Protection: Access control domain on third parties"	
B.17.3 Promoter	Domain is not assessable for this tier. However, the organization should ensure that section A.5.4 (b), (g) and (h) in the Cyber Essentials mark under A.5 Secure/Protect: Access control domain on third parties have been implemented. They should also consider the section on securing your access and environment in CSA's cybersecurity toolkit for SME owners and/or educating your employees on security and securing your access and environment in CSA's cybersecurity toolkit for organization leaders and/or IT teams.	This layer does not need to be assessed for Promoter, but the organization should ensure that appropriate measures are in place for the assessment and monitoring of third-party risks, as detailed in Cyber Essentials mark Section A.5.4 (b), (g) and (h) under "A.5 Security/Protection: Access control domain on third parties"	
B.17.4 Performer	Domain is not assessable for this tier. However, the organization should ensure that section A.5.4 (b), (g) and (h) in the Cyber Essentials mark under A.5 Secure/Protect: Access control domain on third	This layer does not need to be assessed for Performer, but the organization should ensure that appropriate measures are in place for the assessment and monitoring of third-party risks, as detailed in Cyber Essentials mark Section A.5.4 (b), (g) and (h) under "A.5 Security/Protection: Access control domain on third parties"	

	parties have been implemented. They should also consider the section on securing your access and environment in CSA's cybersecurity toolkit for SME owners and/or educating your employees on security and securing your access and environment in CSA's cybersecurity toolkit for organization leaders and/or IT teams.		
B.17.5 Advocate	The organization has established and implemented service level agreements with its third parties to ensure that the third party meets the commitments and expectations on cybersecurity while providing services.	Customers shall set out the relevant requirements for cyber security in the written outsourcing agreement and service level agreement with the Service Provider, including but not limited to: Outsourcing service content; Division of network security rights and responsibilities; Cyber security, data security, and privacy protection requirements; Incident response and reporting mechanisms.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.19-A.5.22.
B.17.6 Advocate	The organization has established and implemented measures to ensure that third parties are informed of their security obligations and to ensure that a security shared responsibility model is established for systems security and data protection; this shall include the organization's CSPs and data center service providers.	Customers shall set out the relevant requirements for cyber security in the written outsourcing agreement and service level agreement with the Service Provider, including but not limited to: Outsourcing service content; Division of network security rights and responsibilities; Cyber security, data security, and privacy protection requirements; Incident response and reporting mechanisms.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.19-A.5.22.
B.17.7 Advocate	The organization has established and implemented measures to assess their third parties before engaging them or on-boarding them to ensure	Customers should responsible for developing the supplier monitoring strategy, including determining the monitoring indicators and monitoring frequency, and conducting continuous monitoring based on the monitoring strategy.	This is the responsibility of tenants. For details about the security

	that they meet all required security obligations based on the risks for the type of services provided by them.	Monitor the extent to which suppliers comply with the organization's security processes and procedures in accordance with the organization's cybersecurity requirements for them. If the organization uses external information systems, cybersecurity requirements should also be imposed on and monitored by the service providers of the external information systems. Customers should responsible for regularly monitoring, reviewing and auditing the services provided by the Service Provider.	practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.19-A.5.22.
B.17.8 Advocate	The organization has established and implemented measures to assess their third parties regularly based on security obligations agreed on systems security and data protection.	Customers should responsible for developing the supplier monitoring strategy, including determining the monitoring indicators and monitoring frequency, and conducting continuous monitoring based on the monitoring strategy. Monitor the extent to which suppliers comply with the organization's security processes and procedures in accordance with the organization's cybersecurity requirements for them. If the organization uses external information systems, cybersecurity requirements should also be imposed on and monitored by the service providers of the external information systems. Customers should responsible for regularly monitoring, reviewing and auditing the services provided by the Service Provider.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.19-A.5.22.
B.17.9 Advocate	The organization has established and implemented measures to ensure that third-party cybersecurity risk management practices such as assessments performed and open risks from third parties engaged are reported to the Board and/or senior management to keep them informed.	Customers should incorporate third-party cybersecurity risk management practices. (e.g., assessments performed and exposures from participating third parties) Regular reporting to management.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.19-A.5.22.

4.1.11 B.18 Vulnerability assessment

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.18.3 Promoter	The organization has established a vulnerability assessment plan with objectives, scope and requirements to review and perform vulnerability assessment on its systems.	Customers should establish a vulnerability assessment plan and perform vulnerability assessment according to the plan's objectives, scope, and requirements to identify potential vulnerabilities in the system. Customers can use **Host Security Service (HSS)** to detect vulnerabilities in Windows/Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provide fix recommendations. (For details, see the product security document on the right.) In addition, HSS provides the vulnerability management function to detect Linux vulnerabilities, Windows vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities. (For details, see the product security document on the right.)	● HSS: Baseline Inspection Overview Detecting and Fixing Vulnerabilities
B.18.4 Promoter	The organization performs regular vulnerability assessment at least on an annual basis to perform non-intrusive scans on its systems to ensure that vulnerabilities are discovered.	The customer should conduct regular security tests, such as penetration tests. Critical ICT systems should be tested and scanned for vulnerabilities on an annual basis. HUAWEI CLOUD provides customers with the **SecMaster service**, which integrates the vulnerability scanning data of **Host Security Service (HSS)** to display the vulnerability risks of cloud assets in a centralized manner, helping customers detect asset security weaknesses in a timely manner and fix dangerous vulnerabilities. (For details, see the product security document on the right.) The vulnerability management function of the SecMaster can scan Linux, Windows, Web-CMS, application, and emergency vulnerabilities, and provide repair suggestions and one-click repair functions (Linux and Windows vulnerabilities) to help customers learn about and fix host vulnerabilities in a timely manner. (For details, see the product security document on the right.)	● SecMaster: Vulnerability Management Overview Policy Management Overview

B.18.5 Performer	The organization has defined and allocated roles and responsibilities for its employees on carrying out cybersecurity vulnerability assessment and management.	Customers should have defined and assigned roles and responsibilities for its employees in performing cybersecurity vulnerability assessment and management, such as vulnerability identification or awareness, vulnerability rating and fixing, vulnerability disclosure and communication, and vulnerability rectification tracking.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 9.2 Vulnerability Management.
B.18.6 Performer	The organization has established and implemented policies and procedures on the requirements, guidelines and detailed steps for conducting cybersecurity vulnerability assessments across its systems to ensure that steps are taken to address the associated risk vulnerabilities identified in a timely manner.	Customers should establish and implement continuous monitoring measures to identify security risks such as security threats and vulnerabilities, and take measures to handle vulnerabilities. Customers can use **Host Security Service (HSS)** to detect vulnerabilities in Windows/Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provide fix recommendations. (For details, see the product security document on the right.) In addition, HSS provides the vulnerability management function to detect Linux vulnerabilities, Windows vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.	● HSS: Baseline Inspection Overview Detecting and Fixing Vulnerabilities
B.18.7 Performer	The organization has established and implemented measures and processes to track, review, evaluate and address the vulnerabilities uncovered as part of the assessments to ensure that the vulnerabilities are being remediated according to their severity.	Customers should responsible for taking necessary measures to identify security vulnerabilities and potential risks periodically or at important time points such as system go-live and change, fixing the detected security vulnerabilities and potential risks in a timely manner or fixing them after evaluating the possible impact, and reporting the vulnerabilities and potential risks to related departments. Security policies, malicious code, patch upgrades, and other security-related matters should be managed centrally. Regularly review and update the effectiveness of personnel, processes, and tools for risk assessment and vulnerability scanning.	● HSS: Detecting and Fixing Vulnerabilities Vulnerability Scan Vulnerability Management Overview Handling Vulnerabilities

		Customers can use **Host Security Service (HSS)** to detect vulnerabilities in Windows/Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provide fix recommendations. (For details, see the product security document on the right.) In addition, HSS provides the vulnerability management function to detect Linux vulnerabilities, Windows vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities. (For details, see the product security document on the right.)	
B.18.8 Advocate	The organization has established and implemented a penetration test plan with the objectives, scope, rules of engagement to ensure that the penetration test can be performed safely.	Customers should develop and implement network security monitoring policies and procedures to detect and report anomalous behavior such as physical or logical intrusions, internal and external threats. Customer can detect asset content compliance, scan the configuration to compare it against the baseline, detect weak passwords, and perform other such functions through HUAWEI CLOUD CodeArts Inspector. HUAWEI **CLOUD Eye Service (CES)** provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take corresponding measures. (For details, see the product security document on the right.) At the same time, HUAWEI CLOUD can also provide an **Advance Anti-DDoS service (AAD)**, **Web Application Firewall (WAF)**, **Database Security Service (DBSS)**, and **Cloud Trace Services (CTS)** to help users accurately and effectively implement comprehensive protection against traffic-based attacks and application level and data-level attacks, as well as reviewing and auditing incidents. (For details, see the product security document on the right.)	● CES: Best Practices of Event Monitoring Cloud Service Monitoring ● AAD: Anti-DDoS Best Practices ● WAF: Best Practices for One-Click Deployment Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN ● CTS: CTS Best Practices CTS Configuring Key Event Notifications
B.18.9 Advocate	The organization performs a regular penetration test at least on an annual basis to discover and exploit security weakness(es) in its systems	Customers should conduct regular security tests, such as penetration tests. Critical ICT systems should be tested and scanned for vulnerabilities on an annual basis.	● HSS: Detecting and Fixing Vulnerabilities

	to ensure that its system's security can be evaluated.	Customers can use **Host Security Service (HSS)** to detect vulnerabilities in Windows/Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provide fix recommendations. (For details, see the product security document on the right.) In addition, HSS provides the vulnerability management function to detect Linux vulnerabilities, Windows vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.	Vulnerability Scan Vulnerability Management Overview Handling Vulnerabilities
B.18.10 Advocate	The organization has established and implemented metrics and thresholds including dashboards to provide reporting and tracking of open, overdue and severe vulnerabilities noted within its systems in order to provide visibility on tracking and remediations within established timelines.	Customers should establish and implement continuous monitoring measures to identify security risks such as security threats and vulnerabilities, and set indicators and thresholds to track and remediate identified or recorded vulnerabilities. Customers can use **Host Security Service (HSS)** to detect vulnerabilities in Windows/Linux operating systems and software such as SSH, OpenSSL, Apache, and MySQL, and provide fix recommendations. (For details, see the product security document on the right.) In addition, HSS provides the vulnerability management function to detect Linux vulnerabilities, Windows vulnerabilities, Web-CMS vulnerabilities, and application vulnerabilities.	● HSS: Detecting and Fixing Vulnerabilities Vulnerability Scan Vulnerability Management Overview Handling Vulnerabilities
B.18.11 Advocate	The organization has established and implemented practices and measures to regularly report on the vulnerability assessment results and findings to the Board and/or senior management.	Customers should report the results of the vulnerability assessment to management.	This is the responsibility of tenants.

4.1.12 B.19 Physical/environmental security

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description

B.19.2 Practitioner	The organization has identified the physical/environmental risks in its environment and implemented detective measures to be alerted on threats to ensure that they are addressed in a timely manner.	Customers should periodically perform risk assessment on the physical places or environments where assets, facilities, and devices are stored to identify threats to the IT environment and analyze the impact of risks. The customer should conduct a risk assessment of the service provider to whom it outsources the work to identify potential risks. Customers should develop and implement risk mitigation and control measures for the identified risks that are consistent with the level of risk tolerance. The disposition of risks should be monitored and reviewed, and the results of the assessment must be formally approved by management.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.3 Practitioner	The organization has performed measures to protect its physical assets against internal and external threats, e.g., the use of cable locks to ensure that they are not stolen or tampered with.	Customers shall implement environmental safeguards based on the criticality of the building, ICT systems and operations. Implement requirements for power supply, temperature and humidity control, firefighting capability, routine monitoring, water supply and drainage, and ESD prevention.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.4 Practitioner	The organization has implemented physical security measures on its perimeters e.g., fence and gate to deter unauthorized access into the premises of the organization.	Customers shall document and implement physical security measures and implement wind, fire, water, and electrical protection measures to prevent unauthorized access and environmental hazards in the data center and sensitive areas.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.5 Promoter	The organization has defined and implemented the process to ensure that visitors are registered and	Customers shall implement physical access controls that authorize individuals by role. Records of access to data centers and sensitive areas should be regularly reviewed to prevent unauthorized access and to	This is the responsibility of tenants. For details about the security

	authorized before having access to the premises of the organization.	ensure that unnecessary access is removed in a timely manner.	practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.6 Promoter	The organization has defined and implemented the process to monitor its premises on a 24/7 basis, e.g., through the use of CCTV to deter and investigate on any physical/environmental threats.	Customers can use the current general equipment room security technology to monitor and eliminate physical hazards. Provide 7*24h closed-circuit television monitoring for the periphery, entrances and exits, corridors, elevators and machine rooms of the machine room, and link with infrared induction and access control.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.7 Promoter	The organization has defined and applied the process to store and transport physical media containing business-critical data securely within and out of its premises to ensure that confidential and/or sensitive data are protected.	Customers should formulate management regulations on storage media and devices entering and leaving the equipment room, and require that storage media and devices must be registered and authorized before entering and leaving the equipment room. Data leakage prevention management is implemented for physical storage media entering and leaving the equipment room. In addition, the data erasure and scrapping processes are specified to reduce possible data leakage losses.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.8 Performer	The organization has established and implemented the policies and procedures on the requirements, guidelines and detailed steps for escalations and security access controls to minimize the impact and interference to its physical environment.	Customers shall implement physical access controls that authorize individuals by role. Access logs to data centers and sensitive areas should be reviewed regularly to prevent unauthorized access.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper>

			6.1 Physical and Environment Security.
B.19.9 Performer	The organization has defined and allocated the roles and responsibilities in detecting, mitigating and responding against physical/environmental risks to ensure that employees are clear of the tasks assigned to them.	Customers shall implement physical access controls that authorize individuals by role. Access logs to data centers and sensitive areas should be reviewed regularly to prevent unauthorized access.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.10 Performer	The organization has established and implemented the policies and procedures on the requirements, guidelines and detailed steps to perform reviews on the physical security measures and assets to ensure that they remain secure.	Customers should develop a physical security policy, including the overall responsibility for physical security, basic physical/environmental security requirements that relevant parties should comply with, and security processes in the physical security domain. The physical security policy should be reviewed and updated periodically or when significant changes occur.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.11 Advocate	The organization has established and implemented policies or processes to report physical/environmental risks and controls to the Board and/or senior management to ensure that they are kept informed of the risks.	Customers should have a policy or process for reporting the results of physical environmental risk reviews and reviews & updates of physical measures to management, and follow the process for reporting to management.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.
B.19.12	The organization has established and implemented a process to review and improve the	Customers should develop a physical security policy, including the overall responsibility for physical security, basic physical/environmental security requirements that	This is the responsibility of tenants. For details

Advocate	physical/environmental security measures to ensure that they are effective.	relevant parties should comply with, and security processes in the physical security domain. The physical security policy should be reviewed and updated periodically or when significant changes occur.	about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 6.1 Physical and Environment Security.

4.1.13 B.20 Network security

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.20.1 Supporter	Domain is not assessable for this tier. However, the organization should ensure that A.2 Assets: Hardware and software domain, A.4.4 (f), (g), (h) and (k) under A.4 Secure/Protect: Virus and malware protection and A.6 Secure/Protect: Secure configuration in the Cyber Essentials mark on network security have been implemented. They should also consider the section on protecting your information assets in CSA's cybersecurity toolkit for SME owners and/or protecting your information assets and securing your access and environment in CSA's cybersecurity toolkit for organization leaders and/or IT teams.	Domain is not assessable for this tier. However, the organization should ensure that they will align to the cybersecurity measures in A.2 Assets: Hardware and software domain, A.4.4 (f), (g), (h) and (k) under A.4 Secure/Protect: Virus and malware protection and A.6 Secure/Protect: Secure configuration in Cyber Essentials mark.	
B.20.2 Practitioner	The organization has configured and implemented access control (e.g., whitelisting, blacklisting) to its	Customers should establish identity and access control policies and implement appropriate technical and management measures to prevent unauthorized access to	• IAM: Custom Policy Use Cases

	network to enforce network security policy and ensure that unauthorized users and/or devices are kept out.	information assets, including remote access mechanisms and log recording. HUAWEI CLOUD **Identity and Access Management (IAM)** Service supports user group-based permission management, allows users to set password policies, password change periods. (For details, see the product security document on the right.) HUAWEI CLOUD IAM supports user group-based permission management, allows users to set login policies, account locking policies, account disabling policies, and session timeout policies that meet customers' status, and provides IP-based ACLs. (For details, see the product security document on the right.)	Recommendations for Using IAM MFA Authentication
B.20.3 Practitioner	The organization has established and implemented the use of stateful firewall over basic packet filtering firewall to ensure that packets are filtered with more context for greater effectiveness.	Customers can use WAF and CFW to protect their resources. HUAWEI CLOUD provides **Web Application Firewall (WAF)** and **Cloud Firewall (CFW)** to help you accurately and effectively defend against traffic attacks, application-layer attacks, and data-layer attacks. (For details, see the product security document on the right.)	● CFW: Best Practices for One-Click Deployment Configuring Inbound and Outbound Access Policies Checking the CFW Dashboard
B.20.4 Practitioner	The network architecture and devices have been reviewed regularly at least on an annual basis to ensure that they are up to date without obsolete rules and protocols.	Customers shall maintain and update its own network architecture diagram, and the team responsible for cyber security shall track and confirm the compliance of the network architecture.	This is the responsibility of tenants.
B.20.5 Promoter	The organization has defined and implemented the process to configure both wired and wireless networks securely, minimally with the use of secure network authentication and encryption protocol and disabling Wi-Fi	CDM runs in user VPCs. Network isolation ensures data transmission security. SSL can be used for data sources that support SSL, such as RDS and SFTP. CDM also supports data migration from public network data sources to the cloud. Users can use VPN and SSL technologies to avoid transmission security risks. (For details, see the product security document on the right.)	● CDM: CDM Migration Principles Enabling Incremental Data Migration

	Protected Setup (WPS) to ensure that the network is secured and data is not lost or breached through the network.	The access information (username and password) for the user data source is stored in the database of the CDM instance and is encrypted using AES-256. (For details, see the product security document on the right.) In scenarios where customers build their own storage, for example, when installing database software on VM instances, it is recommended that customers use the VPC service of HUAWEI CLOUD to build a private network environment, divide network areas by planning subnets and configuring routing policies, and place storage in internal subnets. In addition, network ACLs and security group rules are configured to strictly control network traffic to and from subnets and VMs. (For details, see the product security document on the right.)	Through DataArts Factory ● VPC: VPC and Subnet Planning Suggestions VPC Assess Control
B.20.6 Promoter	The organization has defined and applied a process to carry out network segmentation to segregate into private and public networks with the private network holding all the business-critical data and having no connection to the Internet to ensure that it is isolated from external threats.	Customers are responsible for controlling the communication and data flow within their applications and between their applications and external systems. It is also responsible for authorizing connections to external and internal information systems and recording connection information. For SaaS and PaaS customers, HUAWEI CLOUD allows them to use the VPC service to build isolated production and test environments on the cloud. The **Virtual Private Cloud (VPC)** service provided by HUAWEI CLOUD for customers can create a private network environment for tenants, and realize complete isolation of different tenants in a three-tier network. Tenants have full control over the construction of their own virtual network and configuration, and can configure network ACL and security group rules to strictly control the network traffic coming in and out of subnets and virtual machines, to meet the needs of customers for finer-grained network isolation. (For details, see the product security document on the right.) In addition, customers can different security groups for different types of resources in your VPC. For example, you can isolate OBS resources and RDS instances by associating	● VPC: VPC and Subnet Planning Suggestions VPC Assess Control Private Network Access Network ACL Configuration Examples

		them with different security groups. (For details, see the product security document on the right.)	
B.20.7 Performer	The organization has established and implemented security policies and procedures with the requirements, guidelines and detailed steps to harden the network architecture, device and access security.	The customer shall maintain and update its own network architecture diagram, and the team responsible for network security shall regularly update and enhance the network architecture, equipment, and access security.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper>.
B.20.8 Performer	The organization has defined and allocated roles and responsibilities to oversee, manage and monitor network security to ensure that the employees are clear of the tasks assigned to them.	The customer should establish a cyber security risk management strategy, cyber security policies and procedures, and clearly define and document cyber security roles and responsibilities. Among them, roles and responsibilities for supervising, managing, and monitoring cyber security need to be established and assigned, such as cyber security protection officer, cyber security protection specialist, and cyber security protection office.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Compliance with ISO 27001> A.5.1Policies for information security.
B.20.9 Performer	The organization has established and implemented network intrusion detection on the organization's network to monitor and detect malicious network traffic to ensure that they can be identified and addressed in a timely manner.	Customers shall take measures to prevent and monitor network traffic and protect the system and devices from network intrusion. HUAWEI CLOUD provides **Advance Anti-DDoS (AAD)** and **Web Application Firewall (WAF)** to help you accurately and effectively defend against traffic attacks and application- and data-layer attacks. (For details, see the product security document on the right.) Customers can use the **Virtual Private Cloud (VPC)** service provided by HUAWEI CLOUD to configure network ACLs and security group rules to strictly control the incoming and outgoing network traffic of subnets and VMs and identify possible malicious network traffic. (For details, see the product security document on the right.)	● AAD: Anti-DDoS Best Practices ● WAF: Best Practices for One-Click Deployment ● VPC: VPC and Subnet Planning Suggestions VPC Assess Control Private Network Access

			Network ACL Configuration Examples
B.20.10 Advocate	The organization has established and implemented the policies and processes to evaluate the performance of the network security devices in terms of their effectiveness in blocking malicious traffic and carrying out improvements.	The customer should establish and implement policies and procedures for evaluating the effectiveness of network security devices in blocking malicious traffic, and periodically evaluate the effectiveness and improve the performance. The **Virtual Private Cloud (VPC)** service provided by HUAWEI CLOUD for customers can create a private network environment for tenants, and realize complete isolation of different tenants in a three-tier network. Tenants have full control over the construction of their own virtual network and configuration, and can configure network ACL (For details, see the product security document on the right.) and security group rules to strictly control the network traffic coming in and out of subnets and virtual machines, to meet the needs of customers for finer-grained network isolation. (For details, see the product security document on the right.)	● VPC: Network ACL Configuration Examples Creating a Network ACL Managing Network ACL Tags Associating Subnets with a Network ACL
B.20.11 Advocate	The organization has established and implemented network intrusion prevention on the organization's network to block malicious network traffic and ensure that it is protected from threats.	Customers shall take measures to prevent and monitor network traffic and protect the system and devices from network intrusion. HUAWEI CLOUD provides **Advance Anti-DDoS (AAD)** and **Web Application Firewall (WAF)** to help you accurately and effectively defend against traffic attacks and application- and data-layer attacks. Customers can use the **Virtual Private Cloud (VPC)** service provided by HUAWEI CLOUD to configure network ACLs and security group rules to strictly control the incoming and outgoing network traffic of subnets and VMs and identify possible malicious network traffic.	● AAD: Anti-DDoS Best Practices ● WAF: Best Practices for One-Click Deployment ● VPC: VPC and Subnet Planning Suggestions VPC Assess Control Private Network Access Network ACL Configuration Examples

4.1.14 B.21 Incident response

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description
B.21.1 Supporter	The organization has implemented all the cybersecurity requirements in the Cyber Essentials mark under A.9 Respond: Incident response to ensure that it is ready to detect, respond to, and recover from cybersecurity incidents.	For more information, please refer to cybersecurity measures A.9.4 (a) and (b) in Cyber Essentials mark "A.9 Response: Incident Response".	
B.21.2 Practitioner	The organization has implemented all the cybersecurity recommendations in the Cyber Essentials mark under A.9 Respond: Incident response to ensure they are ready to detect, respond to, and recover from cyber incidents.	For more information, please refer to cybersecurity measures A.9.4 (c) and (d) in Cyber Essentials mark "A.9 Response: Incident Response".	
B.21.3 Promoter	The organization has defined and applied measures to verify the contact details and ensure that the employees involved in the cybersecurity incident response plan are contactable to ensure that they are able to respond in a timely manner.	Customers should develop effective crisis communication measures to inform all relevant internal and external stakeholders in a timely manner. HUAWEI CLOUD has dedicated personnel to keep in touch with industry organizations, risk and compliance organizations, local authorities, and regulatory authorities and establish contact points to ensure timely external support during disaster recovery.	This is the responsibility of tenants.
B.21.4 Promoter	The organization has defined and applied the process to perform cyber exercises to ensure that the stakeholders are involved and know what to do when an incident occurs to ensure that they are well prepared.	Customers should conduct periodic cybersecurity reviews, assessments, tests and exercises to ensure effective identification of cybersecurity vulnerabilities in its systems and organization. HUAWEI **CLOUD Eye Service (CES)** provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to	● CES: Best Practices of Event Monitoring Cloud Service Monitoring

		quickly access warnings regarding cloud resources and take corresponding measures. At the same time, HUAWEI CLOUD can also provide an **Advance Anti-DDoS service (AAD)**, **Web Application Firewall (WAF)**, **Database Security Service (DBSS)**, and **Cloud Trace Services (CTS)** to help users accurately and effectively implement comprehensive protection against traffic-based attacks and application level and data-level attacks, as well as reviewing and auditing incidents.	● AAD: Anti-DDoS Best Practices ● WAF: Best Practices for One-Click Deployment Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN ● CTS: CTS Best Practices CTS Configuring Key Event Notifications
B.21.5 Performer	The organization has defined and applied a process to carry out post-incident review against the cyber exercise or cybersecurity incident to identify areas of improvement and ensure that the incident response plan and process can be strengthened.	Customers should establish a security incident response process to record, respond to, and backtrack security incidents. HUAWEI CLOUD provides **Cloud Trace Services (CTS)** to provide customers with operational records of cloud service resources for user query, audit, and backtracking. **Log Tank Service (LTS)** provided by HUAWEI CLOUD collects, queries, and stores logs in real time. It records activities in the cloud environment, including VM configurations and log changes, facilitating query and tracing.	● CTS: CTS Best Practices CTS Configuring Key Event Notifications ● LTS: Analyzing Huawei Cloud ELB Access Logs for O&M Insights Analyzing Huawei Cloud WAF Logs for O&M Insights
B.21.6 Performer	The organization has defined and established the policies and procedures on the requirements, guidelines and detailed steps to conduct investigation into the incident to gather evidence to ensure	Customers establishes and implements incident and problem management processes to monitor and record operational and security incidents and enable timely recovery of critical business functions and processes in the event of disruption. Events are categorized by appropriate criteria and thresholds, and event alerts are set.	Best Practices of Event Monitoring Cloud Service Monitoring

	that they are able to identify the root cause.	HUAWEI **CLOUD Eye Service (CES)** provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take corresponding measures.	
B.21.7 Advocate	The organization has established and incorporated cybersecurity-related incidents into its crisis management plan to respond against incidents of higher magnitude and impact to ensure that they are treated with the appropriate urgency.	Customers should establish a crisis management plan, incorporate the response, recording, and backtracking processes of cyber security incidents into the plan, and regularly conduct security incident drills and tests.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 9.3 Security Log and Event Management, 9.4 Business Continuity and Disaster Recovery.
B.21.8 Advocate	The organization has established and implemented the policy and process to report cybersecurity incidents and conclude the findings to the Board and/or senior management to ensure that they are kept informed.	Customers should add the feedback process to the security incident response and internal and external communication mechanism, and report the post-event backtracking analysis result of the security incident to the organization management team.	This is the responsibility of tenants. For details about the security practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper> 9.3 Security Log and Event Management, 9.4 Business Continuity and Disaster Recovery.

4.1.15 B.22 Business continuity/ disaster recovery

Clause	Controls	Customers Considering	HUAWEI CLOUD'S Security Best Practice/ Document Description

B.22.2 Practitioner	The organization has identified the critical assets in the organization that require high availability and performed measures to ensure that there are redundancies for them.	Customers should perform a business impact analysis. Quantitatively and qualitatively analyze the risks of serious service interruption, evaluate the key assets that require high availability, and take measures to ensure redundancy. If customers need to back up service data, software, and system images, HUAWEI CLOUD provides multiple products and services with different focuses. For example: Customers can use **Cloud Backup and Recovery (CBR)** to back up cloud servers, disks, file services, off-cloud and VMware virtual environments. Data can be restored to any backup point when data is unavailable due to virus intrusion, accidental deletion, or software/hardware fault. Customers can use the snapshot function of **Elastic Volume Service (EVS)** to restore data to the snapshot point in time when data is lost. Customers can use HUAWEI CLOUD Elastic Load Balance to automatically distribute access traffic to multiple ECSs to expand application service capabilities. HUAWEI CLOUD provides customers with **Storage Disaster Recovery Service (SDRS)** as **Elastic Cloud Servers (ECSs)** and **Object Storage Service (OBS)**, Elastic Volume Service (EVS), and **Dedicated Distributed Storage Service (DSS)** provide disaster recovery functions. Storage Disaster Recovery Service (SDRS) uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide users with high-level data reliability and service continuity. SDRS helps protect service applications by replicating ECS data and configuration information to a DR site. It also allows service applications to start and run properly at the DR site when the servers at the DR site stop, improving service continuity.	● CBR: Using a Custom Script to Implement Application-Consistent Backup CBR Application Case1: Creating an ECS Backup CBR Application Case2: Implementing Automatic Backup for a Vault ● EVS: EVS Snapshot (OBT) Redundant Array of Independent Disks (RAID) ● OBS: OBS Configuring Versioning
B.22.3 Promoter	The organization has defined and applied the process of business impact analysis to identify the critical processes and expected	Customers should conduct a business impact analysis to identify critical services and determine the RTO and RPO of critical services.	This is the responsibility of tenants. For details about the security

	Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for business resumption.	For details about the RTO and RPO, see the best practices in the <HUAWEI CLOUD Security White Paper>.	practices of HUAWEI CLOUD, see <HUAWEI CLOUD Security White Paper>.
B.22.4 Promoter	The organization has defined and applied the process to perform redundancy on systems to ensure the cyber resilience of its systems.	See section B.22.2 for further details	See section B.22.2 for further details
B.22.5 Performer	The organization has established and implemented the business continuity/disaster recovery policies with the requirements, roles and responsibilities and guidelines including the recovery time objectives (RTO) and recovery point objectives (RPO) to ensure that business resumption can be carried out in accordance with the system's criticality.	Customers shall develop a business continuity plan, implement backup and recovery procedures for data and ICT systems based on business recovery requirements (RTO, RPO) and the criticality of the data and ICT systems, and test them regularly. Customers can use the **Cloud Backup and Recovery (CBR)** service of HUAWEI CLOUD to back up data, preventing data loss in the event of a disaster. The CBR service provides permanent incremental backup for customers, shortening the backup duration by 95%. Instant recovery, with a minimum RPO of one hour and a minimum RTO of minutes.	● CBR: CBR Efficient Backup and Recovery
B.22.6 Performer	The organization has established and implemented a business continuity/disaster recovery plan to respond and recover against the common business disruption scenarios including those caused by cybersecurity incidents to ensure cyber resiliency.	Customers should establish and implement incident and problem management processes to monitor and record operational and security incidents and enable timely recovery of critical business functions and processes in the event of disruption. Events are categorized by appropriate criteria and thresholds, and event alerts are set. HUAWEI **CLOUD Eye Service (CES)** provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take corresponding measures. Customers can use **Cloud Backup and Recovery (CBR)** to back up cloud servers, disks, file services, off-cloud and VMware virtual environments. Data can be restored to any	● CES: Best Practices of Event Monitoring Cloud Service Monitoring Resource Group Monitoring ● CBR: CBR Efficient Backup and Recovery

		backup point when data is unavailable due to virus intrusion, accidental deletion, or software/hardware fault.	
B.22.7 Performer	The organization performs regular reviews at least on an annual basis on the business continuity/disaster recovery plan to ensure it is kept up to date.	Customers should regularly test and evaluate their business continuity plans and disaster recovery plans, with the most important measures tested at least once a year to maintain the effectiveness of their recovery strategies.	This is the responsibility of tenants.
B.22.8 Performer	The organization has established and implemented the policy and process to test on its business continuity/disaster recovery plan regularly at least on an annual basis to ensure the effectiveness of the plan in achieving its objectives.	Customers should periodically test the business continuity plan and disaster recovery plan. The test types include desktop drills, functional drills, and comprehensive drills. Plans should be reviewed and updated regularly (at least annually). HUAWEI CLOUD provides customers with the **SecMaster service**. The cloud-native security information and event management (SIEM) solution, which is the security analysis function of the SecMaster service, is used to manage security posture, security information and events, and security orchestration and automatic response. (For details, see the product security document on the right.) Collects management behavior logs of all physical devices, networks, platforms, applications, databases, and security systems and threat detection alarm logs of security products and components, and continuously monitors and analyzes security events in real time. Ensure the effectiveness of business continuity plans. HUAWEI **CLOUD Eye Service (CES)** provides users with a three-dimensional monitoring platform for flexible cloud servers, bandwidth, and other resources. It can help users to quickly access warnings regarding cloud resources and take corresponding measures. (For details, see the product security document on the right.)	● SecMaster Configuring and Enabling a Workflow Configuring Policies ● CES: Best Practices of Event Monitoring Cloud Service Monitoring
B.22.9 Advocate	The organization performs monitoring on the RTO and RPO during business continuity/disaster recovery to ensure that they fall	Customers shall develop a business continuity plan, implement backup and recovery procedures for data and ICT systems based on business recovery requirements (RTO,	● CBR: CBR Efficient Backup and Recovery

	within the targets and report the findings to the Board and/or senior management.	RPO) and the criticality of the data and ICT systems, and test them regularly. Customers can use the **Cloud Backup and Recovery (CBR)** service of HUAWEI CLOUD to back up data, preventing data loss in the event of a disaster. The CBR service provides permanent incremental backup for customers, shortening the backup duration by 95%. Instant recovery, with a minimum RPO of one hour and a minimum RTO of minutes.	
B.22.10 Advocate	The organization performs coordinated business continuity/disaster recovery exercises with its third parties for an extended period of time to evaluate the effectiveness of the processes and procedures.	Customers should incorporate the faults of third-party suppliers into the response and recovery plan. If HUAWEI CLOUD is required to assist the customer in executing the DR plan, HUAWEI CLOUD will actively cooperate with customers.	This is the responsibility of tenants.

4.2 Product Functions

HUAWEI CLOUD provides customers with multiple cloud services to help them establish a cyber security management system and achieve the control objectives in Cyber Trust mark standards. Sort out products that can help customers meet specific requirements by category. One or more products can help meet one or more control requirements. The following table lists the domains in Cyber Trust mark and the products that can help achieve the objectives of the domains. For details about the products, please refer to the **Product Page** on the HUAWEI CLOUD official website.

The following sections describe how some HUAWEI CLOUD flagship products help customers achieve control objectives in Cyber Trust mark.

Cyber Trust mark Control	Products that Help in Achieving the Objectives	Control Requirements that Help in Achieving the Objectives
B.2	**Cloud Eye Service (CES)**	B.2.9
B.8	**Host Security Service (HSS)**	B.8.4、B.8.6、B.8.9
B.9	**Cloud Trace Service (CTS)**、**Data Security Center (DSC)**	B.9.2
	Data Security Center (DSC)	B.9.5、B.9.6、B.9.7、B.9.8、B.9.9
	Data Encryption Workshop (DEW)、**Data Security Center (DSC)**	B.9.11
	Cloud Certificate Manager (CCM)、**SSL Certificate Manager (SCM)**	B.9.12
B.10	**Cloud Backup and Recovery (CBR)**	B.10.3、B.10.4、B.10.10
	Elastic Volume Service (EVS)、**Image Management Service (IMS)**	B.10.5、B.10.6
B.11	**Virtual Private Cloud (VPC)**	B.11.7
B.12	**Cloud Operations Center (COC)**	B.12.3、B.12.6、B.12.10
	Host Security Service (HSS)	B.12.4、B.12.8
	Log Tank Service (LTS)	B.12.5、B.12.9
	SecMaster	B.12.11
	Config	B.12.12

B.13	**Host Security Service (HSS)**、**Advance Anti-DDoS Service (AAD)**、**Web Application Firewall (WAF)**、**Virtual Private Cloud (VPC)**	B.13.3、B.13.4、B.13.7
B.14	**CodeArts**	B.14.6、B.14.8
	Cloud Trace Service (CTS)	B.14.7
B.15	**Identity and Access Management (IAM)**	B.15.3、4、5、7、8、10
	Virtual Private Network (VPN)	B.15.9
	Cloud Trace Service (CTS)	B.15.10
B.16	**Cloud Trace Service (CTS)**	B.16.4
	Log Tank Service (LTS)、**Cloud Eye Service (CES)**	B.16.6
	Cloud Eye Service (CES)、**Web Application Firewall (WAF)**、**Database Security Service (DBSS)**、**Cloud Trace Service (CTS)**、**SecMaster**、**Host Security Service (HSS)**	B.16.7、B.16.9、B.16.11
	Cloud Eye Service (CES)、**Cloud Trace Service (CTS)**	B.16.10
B.18	**Host Security Service (HSS)**、**SecMaster**	B.18.3、B.18.4、B.18.6、B.18.7、B.18.9、B.18.10
	Cloud Eye Service (CES)、**Advance Anti-DDoS Service (AAD)**、**Web Application Firewall (WAF)**、**Database Security Service (DBSS)**、**Cloud Trace Service (CTS)**	B.18.8
B.20	**Identity and Access Management (IAM)**	B.20.2
	Web Application Firewall (WAF)、**Cloud Firewall (CFW)**	B.20.3
	Cloud Data Migration (CDM)、**Virtual Private Cloud (VPC)**	B.20.5、B.20.6、B.20.10
	Advance Anti-DDoS Service (AAD)、**Web Application Firewall (WAF)**	B.20.9、B.20.11
B.21	**Cloud Eye Service (CES)**、**Advance Anti-DDoS Service (AAD)**、**Web Application Firewall (WAF)**、**Database Security Service (DBSS)**、**Cloud Trace Service (CTS)**、**Log Tank Service (LTS)**	B.21.4、B.21.5、B.21.6
B.22	**Cloud Backup and Recovery (CBR)**、**Elastic Volume Service (EVS)**、**Elastic Load Balance**	B.22.2、B.22.4、

	(ELB)、Storage Disaster Recovery Service (SDRS)	B.22.5、B.22.9
	Cloud Backup and Recovery (CBR)、Cloud Eye Service (CES)	B.22.6
	SecMaster	B.22.8

The following table describes the involved HUAWEI CLOUD products.

- **SecMaster**

SecMaster based on cloud-native security, Cloud Brain provides log collection, security governance, intelligent analysis, situational awareness, and orchestration. Provides workspace management, security governance, security posture, asset management, risk prevention, threat operation, security orchestration, data collection, and data integration.

- **Data Security Center**

Data Security Center (DSC) is a next-generation cloud-based data security platform that provides basic data security capabilities, including data classification, data security risk identification, data watermarking for source tracing, and static data masking. DSC integrates the status of each phase of the data security lifecycle in the data security overview to display the overall data security status on the cloud, helping users implement data security management throughout the lifecycle.

- **Host Security Service**

Customers can also use **Host Security Service (HSS)** to comprehensively identify and manage information assets on hosts, monitor risks on hosts in real time, prevent unauthorized intrusions, and build a server security system to reduce major security risks faced by servers. Customers can view and manage the protection status and security risks of all hosts in the same region on the GUI provided by. For host security protection, **Host Security Service (HSS)** of HUAWEI CLOUD implements comprehensive security assessment on the host system. After the assessment, HSS displays the risks of accounts, ports, software vulnerabilities, and weak passwords in the existing system, prompting customers to perform security hardening. This feature eliminates security risks and improves the overall security of the host. HSS also provides the intrusion detection function. When an event such as brute force cracking of accounts, process exceptions, and abnormal logins is detected, an alarm is generated quickly. Customers can learn about alarm events through event management, helping them detect security threats in assets in a timely manner and learn the security status of assets, use intrusion detection to detect and prevent intrusions into the network.

- **Object Storage Service**

Object Storage Service (OBS) provides tenants with massive, secure, reliable, and cost-effective data storage capabilities, such as bucket creation, modification, and deletion as well as object upload, download, and deletion. It can store any type of file and is suitable for websites, enterprises, developers, and common users. As an Internet-oriented service, OBS provides web service interfaces over HTTPS. This enables users to access and manage data stored in OBS anytime and anywhere by using OBS Console or OBS Browser+ on any computer with an Internet connection.

OBS offers a range of access controls — including bucket ACLs, bucket policies, and identity authentication — to restrict access permissions requested by tenants. To keep data storage and access secure, OBS also adopts a series of security measures, such as using access logs for auditing, Cross-Origin Resource Sharing (CORS) for restricting access sources and request types, URL validation to ensure that URLs are from trusted sources, and server-side encryption for keeping data secure.

- **Virtual Private Cloud**

Virtual Private Cloud (VPC) creates an isolated, virtual network environment that users can configure and manage on their own for elastic cloud servers. This enhances the security of user resources on the cloud and makes network deployment easier.

- **Virtual Private Network**

Virtual Private Network (VPN) provides convenient, flexible, and provision-and-play IPsec connections between users' local data centers and Huawei Cloud VPCs, helping build a flexible and scalable hybrid cloud computing environment.

A VPN establishes an encrypted, Internet communications tunnel between a remote user and a VPC. By default, elastic cloud servers on a VPC cannot communicate with the user's data center or private network. The VPN function can be enabled so that they can communicate.

A VPN consists of a VPN gateway and one or more VPN connections. A VPN gateway provides an Internet egress for a VPC and works together with the remote gateway in a local data center. A VPN connection encrypts the communications line between the VPN gateway and the remote gateway and enables communication between the local data center and VPC, quickly establishing a secure hybrid cloud environment.

- **Cloud Certificate Manager**

Cloud Certificate Manager (CCM) is a service that provides certificate issuance and full lifecycle management for cloud services. Currently, it can provide SSL certificate management and private certificate management services. You can purchase SSL certificates from ** and upload local external SSL certificates to the IoT platform for unified management. After deploying the service, customers can replace the HTTP protocol used by the service with the HTTPS protocol to eliminate security risks of the HTTP protocol. This service can be used for website trusted authentication, application trusted authentication, and application data transmission protection.

- **SSL Certificate Manager**

SSL Certificate Manager (SCM) of HUAWEI CLOUD provides customers with one-stop certificate lifecycle management, implementing trusted identity authentication and secure data transmission for websites. The platform cooperates with world-renowned digital certificate authority to provide users with the SSL certificate purchase function. Customers can also upload local external SSL certificates to the IoT platform to centrally manage internal and external SSL certificates. After deploying the service, customers can replace the HTTP protocol used by the service with the HTTPS protocol to eliminate security risks of the HTTP protocol. This service can be used for website authentication, application authentication, and data transmission protection.

- **Identify and Access Management**

Identity and Access Management (IAM) is a user account management service designed for enterprises that allocate resources and operation permissions to enterprise users in a differentiated manner. Once IAM has authenticated and authorized these users, they can use an access key to access Huawei Cloud resources through APIs.

IAM employs a hierarchical fine-grained authorization mechanism to ensure that the users who are part of an enterprise tenant use cloud resources as authorized. This mechanism prevents users from exceeding the scope of their permissions and ensures the continuity of tenant services.

- **Cloud Eye Service**

Cloud Eye Service (CES) is a comprehensive monitoring platform for elastic cloud servers, bandwidth, and other resources. It accurately monitors resource usage, samples indicators in real time, and accurately triggers alarms and notifications based on preconfigured rules. By monitoring alarms, notifications, and custom reports and diagrams in real time, CES enables users to precisely understand the status of service resources. Only tenants that have been authenticated by Huawei Cloud IAM have access to CES, which can be used through the service console, API, command line, or Software Development Kit (SDK). Note that CES does not obtain any tenant data; instead, it monitors only the data related to the utilization of infrastructure resources and such data is isolated by tenant. CES monitors indicators from other cloud services, including ECS, EVS, VPC, RDS, DCS, DMS, ELB, AS, WAF, Workspace, Machine Learning Service (MLS), Data Warehousing Service (DWS), Artificial Intelligence Service (AIS)[1], and more. Alarm rules and notification policies can be set based on these indicators to help users understand the usage and performance status of the instance resources used by each service. CES servers are deployed in a distributed manner to ensure high availability.

- **Cloud Operation and Maintenance Center**

Cloud Operations Center (COC) is a secure, efficient, one-stop, and AI-powered O&M platform to fulfill your centralized O&M requirements. It encompasses Huawei Cloud deterministic operations scenarios and features essential functionalities such as fault management, batch O&M, and chaos drills to improve cloud O&M efficiency while ensuring security compliance.

- **Cloud Data Migration**

Cloud Data Migration (CDM) helps customers migrate homogeneous and heterogeneous data between on-premises and cloud-based file systems, relational databases, data warehouses, NoSQL, big data services, and object storage services.

- **Cloud Backup and Recovery**

Cloud Backup and Recovery (CBR) provides backup protection services for EVS disks, elastic cloud servers, and bare metal servers (EVS disks will be referred to as disks, and elastic cloud servers and bare metal servers will be referred to as servers in subsequent text). It also supports snapshot-based backup services, and can use backup data to restore data on servers and disks. In addition, CBR can synchronize backup data in the offline backup software BCManager, manage backup data on the cloud, and restore backup data to other servers on the cloud.

CBR adopts a microservice architecture, based on which it abstracts and models services. It decouples service data and service logic, platform capabilities and product capabilities, and microservices. Microservices are designed based on the principles of separation between the frontend and backend, stateless services, and interface communication. When interacting with external systems and services, CBR takes into account exceptions such as returned errors, restart, no response, and blocking, and isolates faults to ensure service availability. After faults are rectified, services can be automatically restored.

CBR allows users to create multi-AZ vaults to store backup data in multiple AZs of the same region. When an AZ is unavailable, data can still be accessed from other AZs. This mode applies to scenarios that require high reliability.

CBR controls access based on the IAM service, uses external HTTPS RESTful APIs to protect access channels, uses NTP to ensure time consistency among NEs in the system, and hardens the OS, database, and web application configurations to ensure system security.

CBR supports integrity check of backup data. During backup and restoration, CBR uses CRC32C to verify that backup data is not damaged or tampered with. CBR also supports the backup and restoration of encrypted volumes. After obtaining keys through Huawei Cloud

KMS, CBR backs up encrypted volumes in the production storage to the backup storage, and restores encrypted backup data to the original or new volumes. Backup data of different tenants is stored in different buckets and isolated from each other, protecting user data security to the maximum extent.

- **Cloud Server Backup Service**

If customers want to create online backups, they can use **Cloud Server Backup Service (CSBS)**, it creates consistent online backups for EVS disks on ECSs. If there is a virus intrusion, accidental deletion, or software/hardware fault, data can be restored to any backup point. CSBS works based on the consistency snapshot technology to provide backup service for ECS and BMS, it supports to restore data using data backups, ensuring the security and correctness of user data to the maximum extent and ensuring business security.

- **Storage Disaster Recovery Service**

To meet organizations' requirements for information security and information security management continuity in the event of disasters, **Storage Disaster Recovery Service (SDRS)** provides disaster recovery (DR) protections for ECS, EVS and **Dedicated Distributed Storage Service (DSS)**. SDRS uses multiple technologies, such as storage replication, data redundancy, and cache acceleration, to provide high data reliability and service continuity for users. SDRS protects service applications by replicating the server data and configurations to a DR site. It allows service applications to start at the DR site in the event that servers at the production site stop. This improves service availability and continuity.

- **Web Application Firewall**

Web Application Firewall (WAF) detects HTTP/HTTPS requests. Identifies and blocks attacks, such as SQL injection, cross-site scripting (XSS), web shell upload, command/code injection, file inclusion, sensitive file access, third-party application vulnerability exploits, CC attacks, malicious crawler scanning, and cross-site request forgery, to ensure web service security and stability.

On the WAF console, add a website and connect it to WAF. Then, WAF can be enabled. After this function is enabled, all public network traffic of your website passes through WAF. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server IP address, ensuring that the origin server IP address is secure, stable, and available.

- **Data Encryption Workshop**

Data Encryption Workshop (DEW) is a comprehensive cloud data encryption service that helps address issues in data security, key security, and complex key management. It provides functions such as dedicated encryption, key management, credential management, and key pair management, using the Hardware Security Module (HSM) to protect the security of keys. DEW is integrated with other Huawei Cloud services. Users can use DEW to develop their own encryption applications.

- **Elastic Volume Service、Image Management Service**

Customers can use the snapshot function of **Elastic Volume Service (EVS)** to restore data to the snapshot point in time when data is lost. HUAWEI CLOUD also provides **Image Management Service (IMS)**. Customers can use to back up cloud server instances and use the backup images to restore cloud server instances when the software environment of the instances is faulty. **Cloud Server Backup Service (CSBS)** can create consistent online backups for multiple EVS disks under a cloud server, ensuring data security and reliability and reducing the risk of unauthorized data tampering. **Object Storage Service (OBS)** supports multiple data storage scenarios, customers can also use it for enterprise data backup and archiving.

- **Elastic Load Balance**

Customers can use Huawei Cloud **Elastic Load Balance (ELB)** which automatically distributes access traffic among multiple Elastic Cloud Servers, improving the ability of application systems to provide service and enhancing the fault tolerance of application programs.

- **Database Security Service**

Database Security Service (DBSS) leverages the machine learning mechanism and big data analytics technology to provide functions that ensure database security on the cloud, including database audit, SQL injection attack detection, and risk operation identification. It also provides user behavior discovery and audit, multi-dimensional analysis, real-time alarming, refined reporting, sensitive data protection, and audit log backup.

Database security audit provides the database audit function in bypass mode, enabling the system to generate real-time alarms for risky operations and perform audits. DBSS also generates compliance reports that meet data security standards. In this way, it locates internal violations and improper operations, holding relevant parties accountable.

- **Log Tank Service**

Log Tank Service (LTS) collects logs from hosts and cloud services. By analyzing and processing massive log data, users can maximize the availability and performance of cloud services and applications. LTS provides you with real-time, efficient, and secure log processing capabilities. Helps you quickly and efficiently analyze real-time decisions, manage device O&M, and analyze user service trends.

- **Cloud Trace Service**

Cloud Trace Service (CTS) records operations on cloud service resources so that they can be queried, audited, and traced. Its records operations performed on the management console, executed through an API, and internally triggered on the Huawei Cloud system. CTS is an essential support service for tenant-specific industry certification and IT compliance certification.

- **Advance Anti-DDoS**

Advance Anti-DDoS (AAD) protects servers against large-scale DDoS attacks to ensure reliable and stable services. AAD changes the IP address of a protected server to a high-defense IP address, diverting malicious attack traffic to the high-defense IP address for scrubbing and thereby protecting mission-critical services. It is used to protect Huawei Cloud, non-Huawei Cloud, and IDC Internet hosts.

- **CodeArts TestPlan**

CodeArts TestPlan (formerly CloudTest) is a self-developed one-stop test management platform. It integrates Huawei's years of high-quality software test engineering methods and practices, covering the entire process of test planning, test design, test cases, test execution, and test evaluation. It aims to help enterprises carry out test activities in a collaborative, efficient, and reliable manner to ensure high-quality product go-to-market.

- **CodeArts Check**

CodeArts Check is a self-developed code check service. Based on Huawei's 30-year experience in automatic source code static check technologies and enterprise-level application, Huawei provides users with rich check capabilities, such as code style, general quality, and cyber security risks. It provides comprehensive quality reports and convenient closed-loop problem handling to help enterprises effectively control code quality and facilitate enterprise success.

- **CodeArts Artifact**

CodeArts Artifact is used to manage the build products after source code compilation. Common artifact packages such as Maven, Npm, PyPI, Docker, and NuGet are supported. Seamlessly interconnects with local build tools and continuous integration and deployment on the cloud. In addition, it supports important functions such as artifact package version management, fine-grained permission control, and security scanning, implementing software package lifecycle management and improving release quality and efficiency.

- **CodeArts Deploy**

CodeArts Deploy (formerly CloudDeploy) is an automatic deployment product that supports host, container, and serverless deployment modes. The deployment capability covers multiple languages and technology stacks, such as Tomcat, Spring Boot, Go, NodeJs, Docker, and Kubernetes. Based on the plug-in encapsulation and orchestration capabilities of deployment functions, you can quickly and efficiently release software.

- **CodeArts Build**

Based on large-scale distributed acceleration on the cloud, **CodeArts Build** provides customers with high-speed, low-cost, and easy-to-configure hybrid language build capabilities, helping customers shorten the build time and improve build efficiency.

- **CodeArts Req**

CodeArts Req (formerly ProjectMan) is a requirement management and team collaboration service based on Huawei's years of R&D practice. It has multiple out-of-the-box scenario-based requirement models and object types (requirements, defects, and tasks). It supports multiple R&D modes, such as IPD, DevOps, and lean dashboard. It also provides functions such as cross-project collaboration, baseline and change management, user-defined reports, online Wiki collaboration, and document management.

5 Conclusion

The Cloud Companion Guide for the CSA Cyber Trust mark certification aims to help organizations of all sizes understand how HUAWEI CLOUD services or tools can be used to address the cybersecurity preparedness domains in CSA Cyber Trust mark. By understanding which security services and tools are available on HUAWEI CLOUD, and which controls are applicable to them, customers are able to build secure workloads and applications on HUAWEI CLOUD.

6 Version History

Date	Version	Description
2024-08-30	1.0	First Publication