

HUAWEI TECHNOLOGIES CO., LTD.
Huawei Industrial Base
Bantian Longgang
Shenzhen 518129, P. R. China
Tel: +86-755-28780808
www.huawei.com

Huawei Data Security Governance Practices

Data Security Governance 11/30 Framework



Trademark Notice

HUAWEI, HUAWEI, are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
Other Trademarks, product, service and company names mentioned are the property of their respective owners.

General Disclaimer

The information in this document may contain predictive statement including, without limitation, statements regarding the future financial and operating results, future product portfolios, new technologies, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

Copyright © 2025 HUAWEI TECHNOLOGIES CO., LTD. All Rights Reserved.

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

Huawei Technologies Co., Ltd.
September 2025



CONTENTS

01	Preface	01
02	Huawei Data Security Governance Framework	02
	2.1 Mainline 1: Data Security Governance	03
	2.2 Mainline 2: Data Security Implementation	05
	2.3 Mainline 3: Data Security Engineering Capability	06
03	Huawei Data Security Governance Practices	07
	3.1 Practice 1: Data Security Organization Roles and Responsibilities.....	07
	3.2 Practice 2: Data Security Categorization and Classification	08
	3.3 Practice 3: Huawei Cloud Data Security Practices.....	09
	3.4 Practice 4: HMS Data Security Practices.....	10
	3.5 Practice 5: AI Data Security Governance.....	11
	3.6 Practice 6: Multi-Layer Ransomware Protection for Data Centers	12
	3.7 Practice 7: Cross-Border Data Transfer	14
	3.8 Practice 8: IT Tools for Data Security Management.....	15
04	Afterword	16
05	Appendix: Outline of Huawei's Data Security Governance Framework	17

01 Preface

Global digitalization has accelerated significantly with the rapid advancement of technologies like 5.5G, cloud computing, and AI. This has ushered in a new era of comprehensive connectivity, digitalization, and intelligence, where data has emerged as a key production factor on par with land, labor, capital, and technology. Technological innovation and integration into industries continue to be the key to unlocking the value of data. From the precise control of smart manufacturing to the efficient operation of smart cities, and from differentiated network services to personalized experience, data-driven innovation is reshaping the way we live and work. In particular, AI data—an important part of data—provides powerful support for the development of AI technologies, fosters AI innovation, and drives intelligent transformation across various industries.

However, realizing the value of data must be grounded in security and controllability. Ensuring data security has become a major global challenge, as it affects not only personal information and business interests but also national security and public interests. Recent data security incidents, such as data breaches and ransomware attacks, have disrupted production and services and even caused substantial economic losses and trust issues. These incidents highlight that without secure data flow and use, the digital economy cannot thrive. Ensuring data processing compliance and security is not only a legal requirement, but also the foundation for the success of digital businesses.

To maximize data value and ensure data security, enterprises need to improve their governance systems; build a comprehensive protection framework that covers the entire data lifecycle, from collection, transmission, storage, use, circulation, and cross-border transfer to disposal; and develop data security engineering capabilities. As a global leader in ICT¹ infrastructure and smart devices, operating in over 170 countries and regions, Huawei faces complex and diverse business challenges. Consequently, Huawei adopts a data security governance approach that complies with applicable laws, regulations, and standards while also improving the efficiency of data security practices. The company has systematically analyzed data security laws, regulations, and standards and established a data security governance framework tailored to its unique business needs. Furthermore, it has systematically identified data security control requirements, and developed sets of data security governance controls. These efforts provide guidance for data security initiatives across all business domains and ensure effective long-term data security governance.



¹ ICT: Information and communication technology

02 Huawei Data Security Governance Framework

Huawei respects the data sovereignty of each country and complies with applicable data security laws, regulations, and mandatory standards in each country/region where it operates. The company engages in fair and just market competition globally and is committed to fully protecting customers' data security rights and interests.

When formulating the data security governance framework, Huawei gained insights into global data security laws, regulations, and standards, including:

- **China:** Data Security Law, Network Data Security Management Regulations, Data Security Management Measures in the Industry and Informatization Sectors (Provisional), Data Security Contingency Plan in the Industry and Informatization Sectors (Provisional), GB/T 41479-2022 Network Data Processing Security Requirements, and other data security requirements
- **EU:** Data security clauses in laws and regulations such as Data Act, Digital Services Act, and AI Act
- **International:** Data Management Body of Knowledge (DAMA-DMBOK2) and data security legislation of each country

Huawei decomposes², reorganizes³, and summarizes⁴ these laws, regulations, and standards based on its practices to

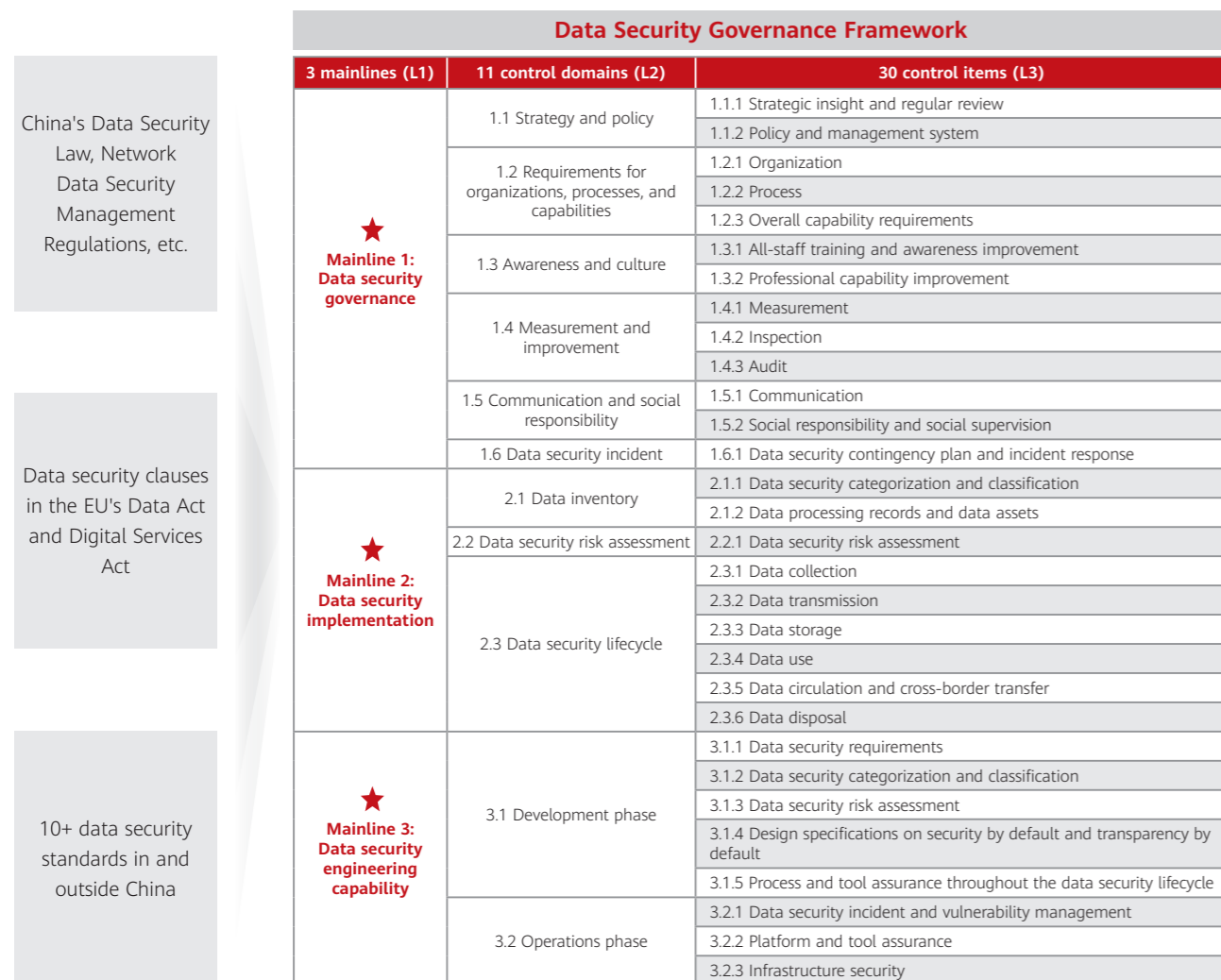


Figure 2-1 Huawei's data security governance framework

establish its data security governance framework. The framework consists of four levels: L1 (mainline⁵), L2 (control domain⁶), L3 (control item⁷), and L4 (specific control measure).

As shown in Figure 2-1, L1 contains three mainlines: data security governance, data security implementation, and data security engineering capability.

- **Mainline 1 "Data security governance":** It covers the top-level design of data security governance and integrates various control domains and items, including policies, organizations, awareness education, measurement, and incident response.
- **Mainline 2 "Data security implementation":** It covers data inventory, risk assessment, and data management requirements throughout the lifecycle, from collection, transmission, storage, use, circulation, and cross-border transfer to disposal.
- **Mainline 3 "Data security engineering capability":** It covers the data security engineering capabilities required for the product/service development phase and the operations phase of data processing.

These three mainlines (L1) comprise 11 control domains (L2), 30 control items (L3), and 84 control measures (L4). The control measures will be reviewed regularly and their quantity may change. Given that Huawei already has a privacy governance framework, its data security governance framework focuses on the legal and regulatory requirements for important data, as well as additional requirements for personal information protection (e.g., a data security owner must be designated and a data security management organization must be established when personal information of over 10 million people is processed).

The following describes the control domains (L2) included in the three mainlines (L1).

2.1 Mainline 1: Data Security Governance

This mainline lists the general control domains led by the governance team (not business department-specific). It encompasses the following:

1. Strategy and policy

This control domain outlines specific requirements for understanding external data security requirements (in laws, regulations, and standards) and translating them into internal data security management systems. It also covers the formulation, updating, and maintenance of data security management regulations. Huawei's business groups/units (BGs/BUs) promptly update their data security management systems (or integrate requirements into existing cyber security and privacy management systems), processes, practices, and guidelines. These updates are made in accordance with the data security requirements in this control domain and relevant laws, regulations, industry standards, and best practices regarding data processing, ensuring the BGs/BUs can adapt to new situations.

² Decomposition, also known as slicing, involves breaking down selected laws, regulations, and standards into standalone clauses. Each clause is supplemented with contextual details (Who, When, Where, What, and How) to ensure it can be applied independently.
³ Reorganization refers to grouping all relevant clause requirements that apply to the same scenario (mapped to L3) into unified controls (mapped to L4) while identifying original sources. The merged controls include overlapping or similar requirements for the same scenario from different external frameworks, and they serve as input for further summarization.
⁴ Summarization involves distilling the reorganization results into actionable controls that can be implemented by business teams.
⁵ Mainline refers to the primary basis for classifying controls (based on the division of control implementation responsibilities) and is used to describe the level-1 catalog (L1) of control sets.
⁶ Control domain refers to the domain to which controls are applicable and is used to describe the level-2 catalog (L2) of control sets.
⁷ Control item refers to the specific item to which a control is applicable and is used to describe the level-3 catalog (L3) of control sets.

2. Requirements for organizations, processes, and capabilities

This control domain defines the overall requirements for organizational structures, processes, and capabilities, and provides guidance for designing data security organizational structures, formulating process guidelines, and developing capabilities. To meet the requirements of this control domain and its associated control items, Huawei has established a data security management organization and appointed data security owners in each business domain.

3. Awareness and culture

This control domain aims to improve employees' data security awareness and capabilities, and provides guidance on the planning, content development, and evaluation of data security training. Huawei already conducts regular data security awareness training for all employees and capability training for professionals, and tracks and evaluates training.

4. Measurement and improvement

This control domain encompasses requirements for measurement, inspection, and auditing. Huawei has established a three-level supervision mechanism, which includes self-checks within BGs/BUs, measurements and inspections conducted by data security teams, and audits. Findings from these activities are managed and resolved to facilitate continuous business improvement.

5. Communication and social responsibility

This control domain encompasses requirements for submitting relevant reports (e.g., data security risk assessment reports) to regulators, fulfilling social responsibilities, and undergoing public oversight. It also involves sharing data security practices within the industry and contributing to the development of international and national standards.

6. Data security incident

This control domain encompasses requirements for data security incident emergency plans, emergency exercises, incident response, and incident reporting. Huawei's BGs/BUs carry out regular emergency exercises on data security incident response.



2.2 Mainline 2: Data Security Implementation

This mainline outlines the set of controls that need to be implemented by business departments that process data. It encompasses the following:

1. Data inventory

This control domain provides data security guidance on data security categorization and classification, data processing records, data asset inventories, and other aspects to ensure the integrity and accuracy of data processing records. Each BG/BU maintains the processing records of high-risk and high-value data (including basic information about data processors, processing purposes, safeguards, entrusted processing, and cross-border transfer) in line with the requirements of this control domain.

2. Data security risk assessment

This control domain outlines the requirements for conducting data security risk assessments (including routine reviews) and specifies the content to be covered. Huawei's BGs/BUs integrate such assessments into business processes for high-risk and high-value business scenarios, conduct these assessments to identify potential threats and risks in business scenarios, and take appropriate measures to address risks.

3. Data security lifecycle

This control domain defines data security lifecycle phases and data protection requirements in each phase. The phases include the following, for which BGs/BUs take responsibility:

- **Data collection:** Specifying the data collection purpose, scope, and source, along with security measures. For data used in AI training, both data and data sources must be identified and documented.
- **Data transmission:** Specifying security configurations for data transmission channels, cryptographic algorithms, digital certificates, key protection, and other requirements.
- **Data storage:** Specifying requirements for secure data storage, access control, archiving, and data backup and recovery.
- **Data use:** Specifying the scenarios where data use is prohibited, and the preprocessing and governance requirements (including labeling, ensuring diversity, preventing discrimination, and making corrections) for data used in AI training; specifying transparency requirements for advertising services, and the need to provide options that are not based on personal characteristics during personalized recommendations.
- **Data circulation and cross-border transfer:** Specifying contractual requirements for entrusting third parties to process data, third-party supervision and management obligations when providing network platform services, data protection obligations when we are entrusted to process data and provide external services, cross-border data transfer mechanisms, and the requirements that must be met when the corresponding transfer mechanism is used.
- **Data disposal:** Specifying the requirements for securely disposing of data assets that have expired or lost their value (by means of deletion, masking, destruction, or others).

▶ 2.3 Mainline 3: Data Security Engineering Capability

This mainline lists the engineering capability requirements (e.g., specifications, technologies, components, or tools) required for each data processing activity, including:

1. Development

This control domain outlines the data security engineering assurance capabilities required for product, solution, and service development, including:

- **Data security requirements:** The security competence center specifies the priority of data security requirements, requirement document content, and mechanisms for documenting and reviewing requirement analysis reports.
- **Categorization and classification:** The center develops data security categorization and classification rules, templates, or tools. It establishes rules in line with the principle of "categorization comes before classification." Categorization is based on the business-relevant industry, data categories (if any) established by the competent department in the industry, and business attributes. Classification is determined by data impact analysis results (impacts of data breaches on national security, corporate rights and interests, and individual rights and interests).
- **Data security risk assessment:** The center develops data security risk assessment methods, templates, or tools. They can be used to evaluate whether products' security by default, privacy by default, and transparency by default ensure data security and protect the rights and interests of relevant stakeholders. They can also help business departments conduct basic security assessments and data lifecycle security assessments on data processing activities to identify risks.
- **Design specifications on security by default and transparency by default:** The center specifies the design requirements for identity authentication, permission management, access control, log recording, data protection, and transparency.
- **Process and tool assurance throughout the data security lifecycle:** This includes technical solutions and transparency design for notification and consent obtaining before data collection; cryptographic infrastructure (e.g., digital certificates and key management systems) required for data transmission and storage, data cleansing (deletion or de-identification), labeling, rectification, error correction, and data quality evaluation before data use; necessary tools required for data circulation and cross-border transfer; and data disposal methods (e.g., anonymization) and tools.

2. Operations

This control domain outlines the data security engineering assurance capabilities required in the operations phase of products, solutions, and services, including:

- **Data security incident and vulnerability management:** This includes data security incident classification criteria, risk monitoring and warning (e.g., traffic analysis and intrusion detection), emergency response capability, and processes and tools that support incident response and vulnerability management.
- **Platform and tool assurance:** This includes data security governance systems or tools (e.g., data inventory management, data asset management, and metadata management), data security assurance systems or tools (e.g., identity authentication, permission management, encrypted storage, and key management systems), and security O&M tools (e.g., log analysis and security detection).
- **Infrastructure security:** This includes data security of network access devices, network availability and security defense, and cloud environment data security (implementation of security policies and responsibility mechanisms that are consistent with those in traditional computing environments).

03 Huawei Data Security Governance Practices

Huawei's data security governance framework has been integrated into the operational processes of major business domains. This integration has led to the formation of relevant organization roles, typical governance activities, guidelines, and IT tools. The data security governance practices encompass:

- **Organization roles and typical governance activities:** Data security organization roles and responsibilities, AI data security governance practices, cross-border data transfer practices, and data security built into the Huawei Mobile Services (HMS) process.
- **Guidelines:** Data security categorization and classification methods.
- **IT tools:** IT tools for data security management, providing data inventory, risk assessment, measurement, and compliance evidence.

Huawei's main data security governance solutions and tools have been integrated into data security products and solutions, including:

- **Data security products:** Data security center (provided by Huawei Cloud to improve customers' data security level) and data security management SaaS IT tools (providing data inventory, risk assessment, measurement, and compliance evidence).
- **Ransomware protection solution:** Multilayer Ransomware Protection (MRP) provided by ICT Product Portfolio Mgmt & Solutions Dept to safeguard against data ransomware threats.

These products and solutions make it easier for customers to implement data security governance and manage and measure data security, enhancing their data security governance levels.

▶ 3.1 Practice 1: Data Security Organization Roles and Responsibilities

Huawei's data security organization roles and responsibilities are as follows:

- **Primary data security owner:** Each BG/BU director serves as the primary data security owner, who is responsible for ensuring adequate personnel, budget allocation, and capability development.
- **Data security management owner:** This role is designated in each BG/BU and is responsible for data security compliance and risk management.
- **Data security management organization:** This organization is responsible for the framework, basic principles, and requirements of data security management, and supports the implementation of these requirements. The data security management organization in each BG/BU is responsible for establishing and maintaining its data security management requirements, incorporating them into processes, and responding to regulators' supervision and inspection. The data security management organization in the region/country where the business is operating is responsible for identifying local data security laws and regulations and incorporating data security requirements into local compliance guides. Businesses can also establish separate data management organizations to meet their business needs. These organizations are responsible for developing and promoting the data management framework, process specifications, methods, and tools, and supporting the implementation of data security management requirements.

3.2 Practice 2: Data Security Categorization and Classification

Data security categorization and classification form the foundation of data security governance. It is essential to identify sensitive data and valuable data assets, and to designate data asset owners.

Data security categorization is based on business processes (e.g., integrated product development, procurement, supply, marketing, and service & delivery) to establish the data category catalog. BGs/BUs can further categorize data based on their process information architecture to refine the data category catalog.

Data security classification is determined by data impact analysis results. Specifically, it is defined by the impacts that data breaches have on national security, corporate rights and interests, and individual rights and interests when the data confidentiality, integrity, availability, and compliance (with applicable laws, regulations, contracts, or agreements throughout the data lifecycle) are compromised. Data is classified into four levels (L4, L3, L2, and L1) in descending order of impact severity.

Level	Data Classification Description
L4	<ul style="list-style-type: none"> Core data⁸ Sensitive personal information, such as biometric information
L3	<ul style="list-style-type: none"> Important data⁹ Other personal information (e.g., communication records, recordings/videos in non-public circumstances, personal mobile numbers, and home addresses) that could pose significant risks to individual rights and interests if compromised
L2	<ul style="list-style-type: none"> General data with potential risks Personal information (e.g., names) that generally impacts individual rights and interests
L1	<ul style="list-style-type: none"> Data with no risk or minor impact Personal information (e.g., employee IDs) that is essential for HR management in office settings and poses minor impacts on individual rights and interests, and personal information (e.g., MAC addresses of personal devices) that is less relevant to personal identifiability

Table 3-1 Data classification

If multiple factors—for example, national security, corporate rights and interests, and individual rights and interests—are affected, each BG/BU can select an appropriate data classification and control implementation solution for its business scenarios:

- Solution 1:** Multi-label classification is used to retain multiple data classification results so that appropriate controls can be taken. The controls implemented in this solution include only data classification ones (they incorporate controls for different data categories stipulated in laws and regulations).
- Solution 2:** Data classification follows a "highest-level-prevails" principle. The controls implemented in this solution include both data security categorization and classification measures. Data classification controls primarily consist of technical safeguards and organizational measures, including storage encryption, transmission encryption, de-identification display, and internal permission control. Data security categorization controls are mainly compliance requirements for the involved data categories stipulated in applicable laws and regulations. Such requirements include obtaining separate consent from personal information subjects for processing their sensitive personal information.

⁸ According to GB/T 43697-2024 Data Security Technology – Rules for Data Classification and Categorization, core data refers to key data that either has a high coverage in a specific sector, group, or area or that has reached a high level of precision, scale, and depth and once unlawfully used or shared, may pose a direct threat to political security.

⁹ According to China's Data Security Law, important data refers to data that either belongs to a specific sector, group, or area or that has reached a certain level of precision and scale and once tampered with, damaged, leaked, or unlawfully obtained or used, may directly endanger national security, economic operation, social stability, or public health and security.

3.3 Practice 3: Huawei Cloud Data Security Practices

Huawei Cloud leverages its data security engineering capabilities (indicated in mainline 3) to develop products, significantly improving customers' data security. For example, Huawei Cloud safeguards the data of a financial management platform in China by providing the following data security solutions:

- Data security center (DSC):** provides capabilities such as sensitive data identification, categorization and classification, asset catalog, watermarking for source tracing, and static data masking.
- Encryption gateway:** works with the key management system (KMS) to implement data encryption.
- Application security gateway:** provides data discovery, security protection, data masking, auditing, and other capabilities.
- Data leakage prevention (DLP):** provides content identification, operation interception, audit recording, and other capabilities.
- O&M audit:** supports host O&M and database audits.

These solutions significantly enhance customers' data security and provide a solid foundation for customers to pass Multi-Level Protection Scheme (MLPS) level-4 and cryptography assessment level-3 certifications.

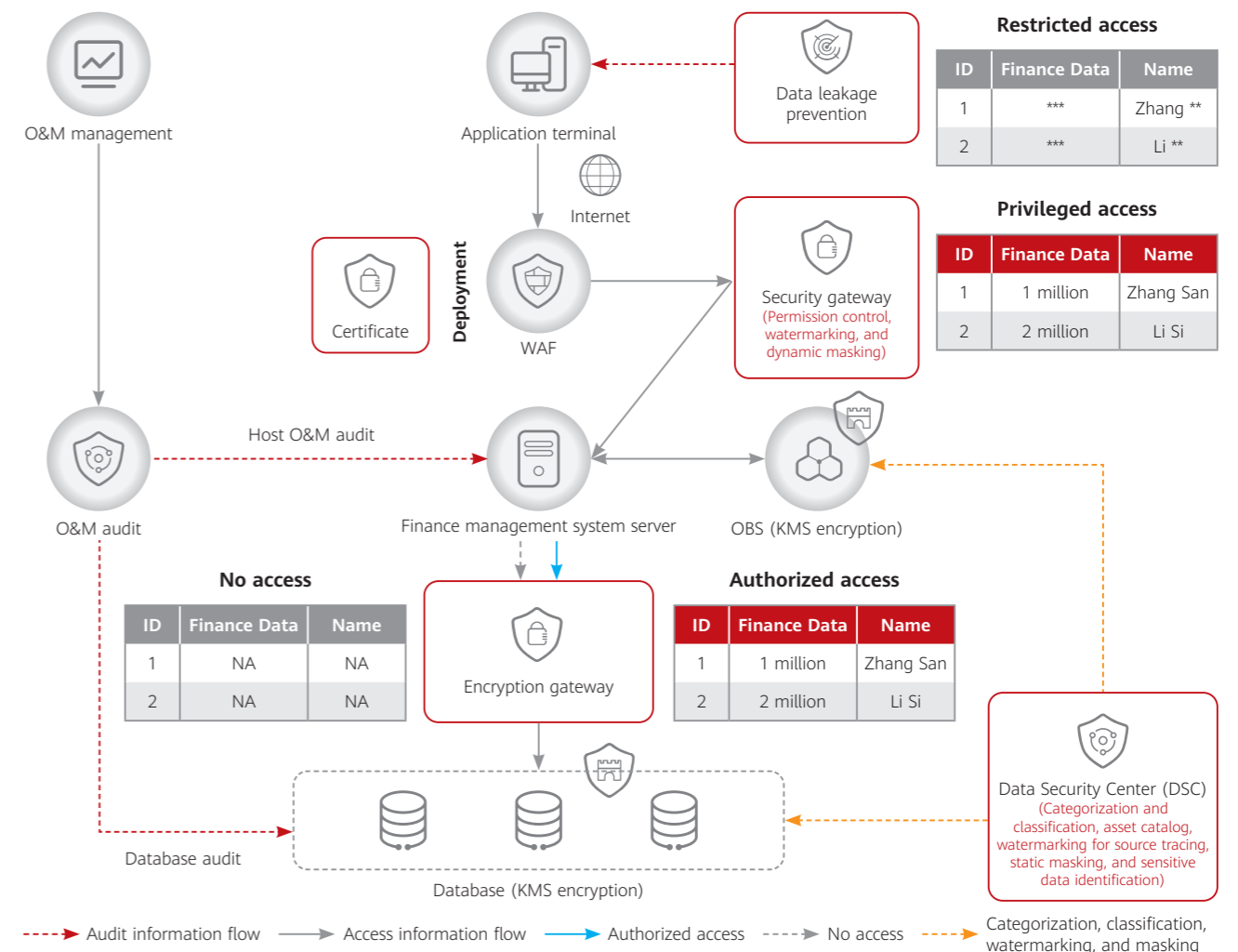


Figure 3-1 Data security capabilities provided by Huawei Cloud

DSC offers essential data security capabilities, including data security categorization and classification, data masking, data watermarking, and data protection. It provides asset maps to present the overall data security situation on the cloud, and supports one-stop data security operations. Additionally, DSC enhances AI data security and privacy compliance capabilities to meet the new requirements of AI models, and ensures data security and privacy compliance during AI training and inference.

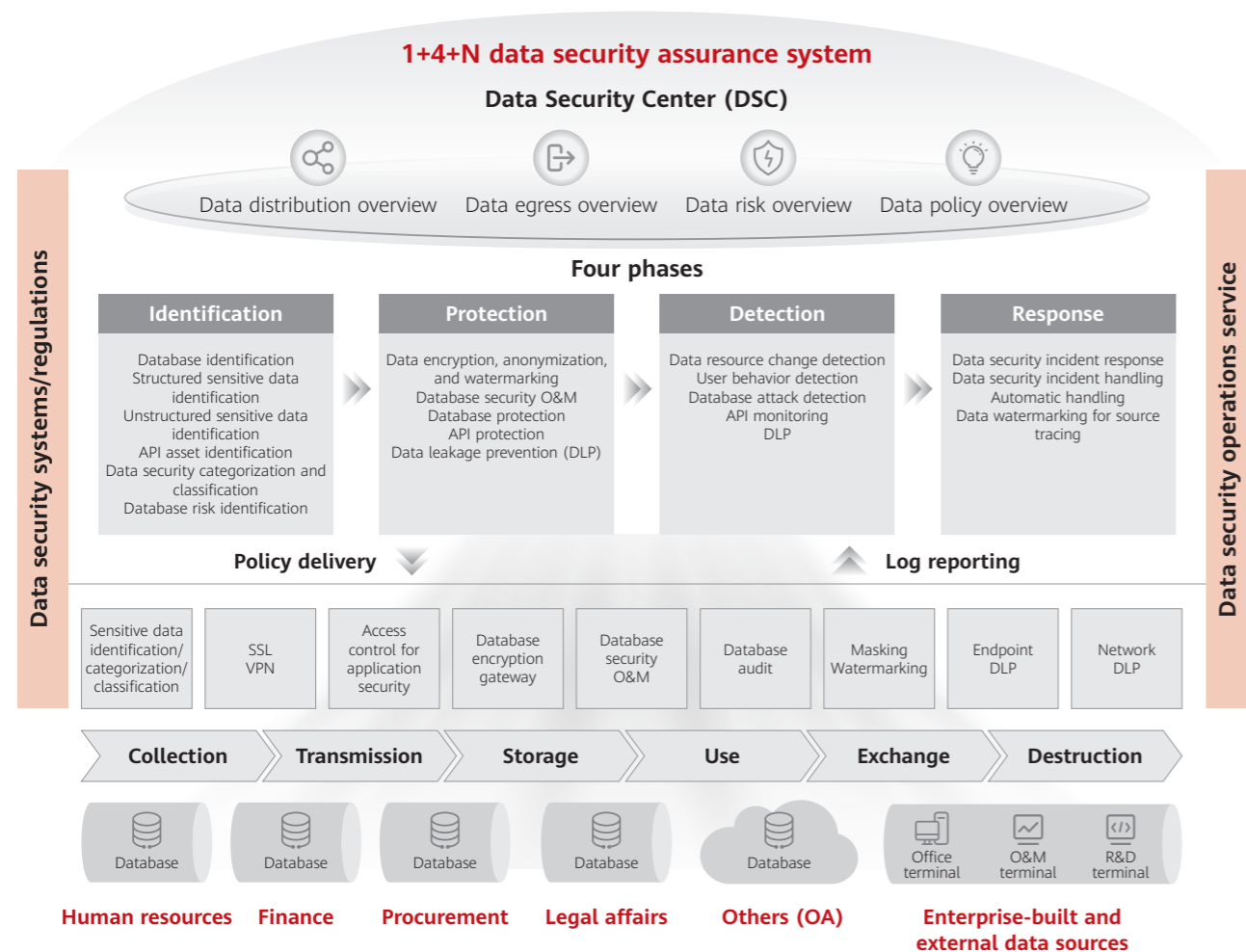


Figure 3-2 Overview of DSC capabilities

Huawei Cloud's data security assurance system includes:

- **One center:** DSC manages data security and provides unified security protection, security policies, and log analysis.
- **Four phases:** A resilient data security system is built in the identification, protection, detection, and response phases.
- **N scenarios:** Various scenarios and data sources are supported.

3.4 Practice 4: HMS Data Security Practices

Serving as the "brain" of Huawei smart devices, HMS provides cloud service support for devices, and delivers a high-quality digital experience across all user scenarios, including data, applications, travel, and entertainment. These services help enhance users' digital lifestyles.

HMS has set 10 key control points (KCPs) for data security in its service process, involving different control domains in mainline 2, namely, data inventory, risk assessment, and data security lifecycle. These KCPs are as follows:

1. Key roles in the data domain
2. Data asset catalog
3. Data access compliance
4. Data retention compliance
5. Data security categorization and classification
6. Tag lifecycle management
7. Privacy compliance in personal data/big data operations
8. Data storage security
9. Permission control
10. Data sharing

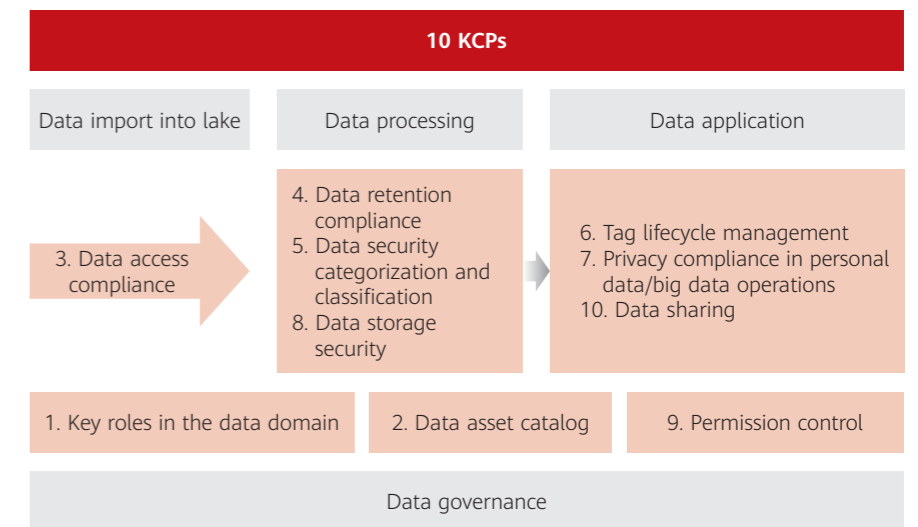


Figure 3-3 HMS data security KCPs

At these KCPs, HMS teams implement digital internal controls primarily through measurement, including:

- Identifying risks throughout the data lifecycle, measuring the effectiveness of these KCPs through metrics, verifying the effectiveness of control execution, and checking whether the preset security policies meet intended objectives to prevent improper execution.
- Identifying abnormal data in key metrics to pinpoint weaknesses (e.g., low categorization and classification rates or excessively long data retention periods) in controls, and helping quickly locate issues and optimizing controls (including rectification, supplement, and adjustment).
- Retaining records of findings, improvements, audit logs, and audit reports to facilitate continuous improvement and demonstrate that security mechanisms can ensure continuous security during certification and audit activities.

These process development and continuous measurement practices enable prompt detection and resolution of issues, effectively ensuring data security and processing compliance.

3.5 Practice 5: AI Data Security Governance

AI data security is a typical business scenario of data security governance. Under the data security governance framework, Huawei implements a series of measures to ensure data processing compliance and data lifecycle security. The measures include:

1. **AI data security governance:** Huawei establishes and improves the AI data management mechanism, develops AI data security specifications and guides, and incorporates these specifications into the AI data and model development process. Furthermore, the company refines AI data categorization and classification, and specifies the processing rules and security requirements for different categories of data. In addition, it establishes and improves the data security standards of AI datasets, specifies the owners and output requirements of each process node, and ensures that only data that meets the data security standards can be used for model training.
2. **AI data security implementation:** During the AI data planning and design phase, Huawei verifies data sources and their validity to ensure compliance. In the raw data preprocessing phase, Huawei scans for high-risk data (including intellectual property and personal information). This is performed to prevent processing data with intellectual

property risks, with unnecessary personal information being deleted or de-identified based on business purposes, thereby protecting intellectual property and the rights and interests of personal information subjects. For AI data, models, and products integrated with AI models, Huawei performs data impact assessments (including personal information impact assessments) in accordance with applicable laws and regulations in relevant countries/regions.

3. AI data security engineering: Huawei has developed a comprehensive data toolchain to manage AI datasets and versions in a unified manner and enabled traceability between datasets and models. The company continues to enhance its AI data processing platform by integrating identification rules and scanning tools for sensitive information in different countries/regions, and integrating detection and cleansing tools for data related to intellectual property rights (IPR). Huawei has also built data security safeguards, including topic limitations and keyword detection.

By adopting the data security governance framework in the AI data security field, Huawei strengthens its overall governance of AI data, safeguards the security of such data, and protects the legitimate rights and interests of all stakeholders.



3.6 Practice 6: Multi-Layer Ransomware Protection for Data Centers

Ransomware has become increasingly sophisticated over the past few years, evolving rapidly and updating more frequently. The number of attacks has surged exponentially, with encryption speeds becoming faster than ever. And the range of targets has expanded significantly. On average, a ransomware attack hits an organization every 11 seconds. When successful, such an attack typically disrupts services for over five days. Traditional ransomware protection methods, which rely on behavior, feature, and network flow detection (network security + storage backup and recovery), are no longer sufficient to handle the growing complexity of these threats. Huawei's innovative MRP technology addresses this by enabling network-storage synergy to build dual digital security protection. On the network side, MRP accurately identifies ransomware and other viruses, preventing lateral threat propagation. And on the storage side, this technology provides the final line of defense for data security, ensuring service recovery. With network-storage synergy, MRP effectively protects customer data security through three core capabilities: accurate identification, comprehensive protection, and rapid recovery.

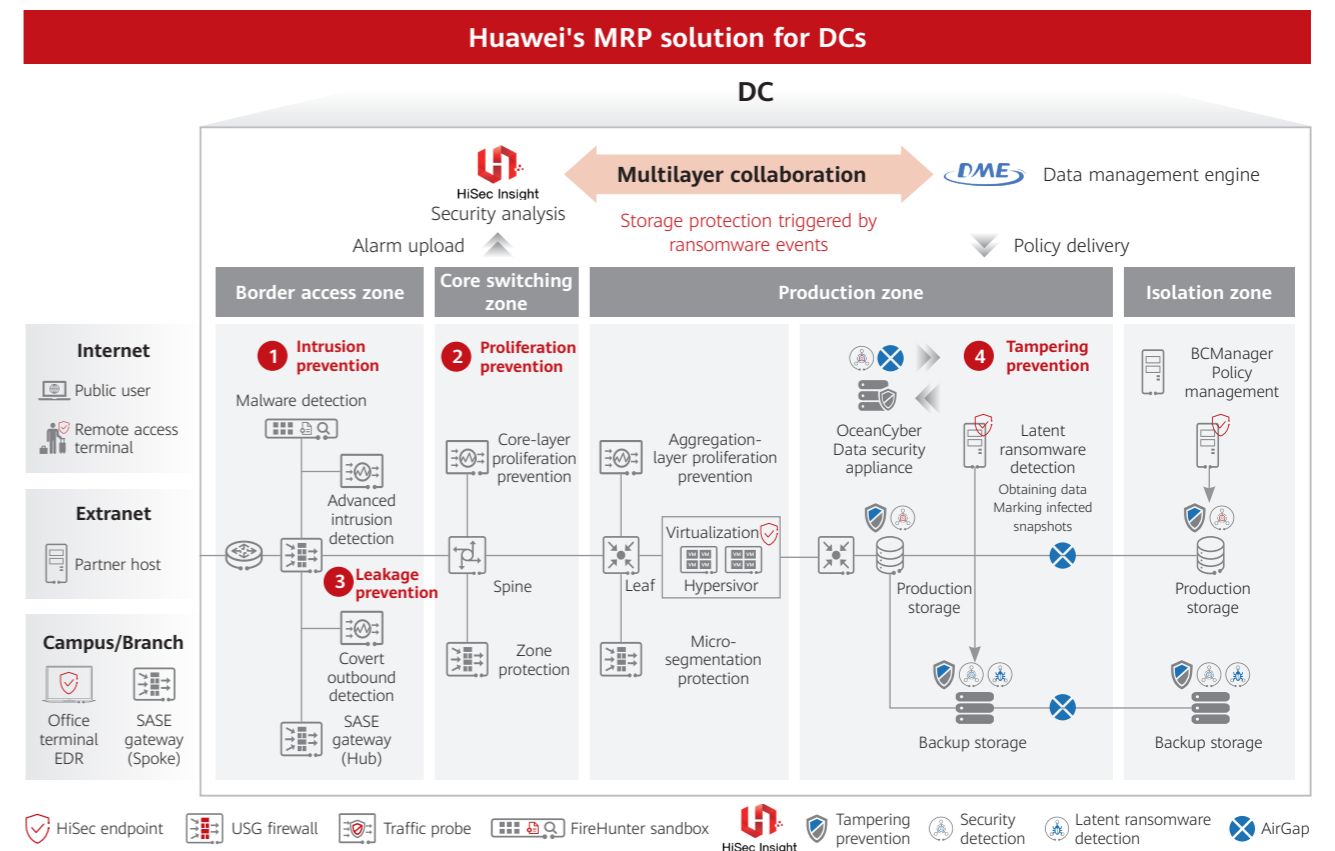


Figure 3-4 MRP

Using technologies such as intrusion, proliferation, and leakage prevention (indicated by ①, ②, and ③), MRP provides comprehensive data ransomware protection with proactive, in-depth defense. It automatically blocks attack entry points through devices' intrinsic security mechanisms, network-side high-risk vulnerability blocking, and EDR-based¹⁰ phishing email detection. NDR¹¹ and EDR are deployed to accurately detect and quickly handle intranet lateral movements that bypass IPS, including remote control, brute force cracking, and ransomware encryption. NDR is used to identify covert data sending on the network side, while EDR is used to identify encrypted data leakage by ransomware families on the endpoint side and detect DLP¹² bypass data theft. Furthermore, HiSec Insight collects ransomware alarms from the live-network SIEM¹³/SOC¹⁴/situation awareness systems, triggers protection through interworking with DME¹⁵, and supports compatibility with heterogeneous devices.

With the tampering prevention function (marked in ④), MRP ensures data security and provides assured RPO¹⁶. Serving as the final line of defense, the storage-side ransomware protection solution offers three key protection mechanisms: anti-tampering, encrypted file security detection, and isolation zone. The isolation zone uses an air gap to disconnect replication links when inactive, protect online assets from attacks, and assure RPO. With these protection mechanisms, MRP prevents ransomware and other viruses from altering data.

Network security and storage devices work together to ensure that the backup data RPO can be achieved within minutes.

¹⁰ EDR: Endpoint Detection and Response
¹¹ NDR: Network Detection and Response
¹² DLP: Data Leakage Prevention
¹³ SIEM: Security Information and Event Management
¹⁴ SOC: Security Operations Center
¹⁵ DME: Data Management Engine
¹⁶ Recovery Point Objective (RPO) indicates the maximum amount of lost data that can be tolerated by the system.

When low-risk (e.g., ransomware interception), medium-risk (e.g., ransomware spreading), or high-risk (e.g., ransomware encryption) ransomware events are detected on the network side, proactive data protection can be triggered. The protection measures include one-time, medium-frequency, and high-frequency secure snapshots in primary storage, as well as one-time secure backups. A noteworthy point here is that frequent linkage triggering does not affect services.

The collaboration between network security and storage devices ensures that backup data is not contaminated. This solution can accurately detect ransomware and other latent malware in compressed backup data, automatically flag infected files, and prevent these files from being restored. In the event of a high-risk ransomware event (e.g., ransomware encryption), the air gap is activated to halt data replication within the replication window to contain the threat.

HiSec Insight collects ransomware alarms from storage devices to accurately detect ransomware attacks. It also collects such alarms (e.g., file encryption alarms) from primary storage and backup devices to detect ransomware attacks that bypass security protection measures on the live network.

The MRP solution has been successfully applied in the finance, manufacturing, government, and electric power industries. With isolation zone and network-storage synergy, it can ensure that RPOs are achieved within minutes and that backup data is not contaminated.

▶ 3.7 Practice 7: Cross-Border Data Transfer

Organizations must implement local deployment measures when local storage is mandated by laws and regulations. In scenarios where cross-border transfer is allowed under certain conditions, organizations must meet these conditions before proceeding with such transfers. The following five steps can help organizations to achieve this:

- 1. Identify and track the legal and regulatory requirements and changes in relevant countries/regions:** This step is primarily handled by the legal affairs and data security teams. These teams review the laws and regulations, learn about their control scopes and specific requirements for cross-border data transfers in relevant countries/regions, and specify available data transfer tools (also known as cross-border transfer mechanisms, such as assessment, certification, and standard contracts).
- 2. Maintain records of cross-border data flows:** Such flows are associated with business and IT information flows. Business departments maintain comprehensive records of cross-border data flows, with support from the IT, legal affairs, and data security teams, and regularly review and update them to adapt to business.
- 3. Select appropriate cross-border transfer tools:** Select appropriate tools in line with relevant rules in the countries/regions where data exporters are located. Take the standard contractual clauses (SCC) as an example. Key areas of focus include whether the importing country's data protection environment assessment and restrictions are involved, which requirements must be met, whether the data importer's technical and organizational measures align with the SCC, and whether the data transfer agreement signed between the data exporter and importer needs to be filed.
- 4. Comply with the legal and regulatory requirements associated with cross-border transfer tools.** For instance, if the SCC is used, perform a transfer impact assessment. If the assessment is successful, draft a cross-border transfer agreement in accordance with the SCC, get the related parties to sign the agreement, and file with the local data protection authority if required. Conversely, if the assessment fails, revert to the previous step. In cases where there is no suitable cross-border transfer tool, consideration should be given to deploying IT systems locally.
- 5. Fulfill contractual obligations of cross-border data transfer and conduct regular reviews and assessments:** Adhere to the signed cross-border data transfer agreement and take necessary technical and organizational measures to protect cross-border data. Regularly reassess cross-border data transfers to minimize unnecessary transfers and enhance data protection in different scenarios.

Among the preceding five steps, accurate recording of cross-border data flows is crucial. Huawei primarily uses the data security management IT tools described in practice 8 to record, track, and maintain these data flows.

▶ 3.8 Practice 8: IT Tools for Data Security Management

Huawei has developed IT tools for data security management under its data security governance framework. These tools provide a wide range of functions—including data security categorization and classification, important data inventory templates, and data security risk assessment templates—to help business departments meet legal and regulatory requirements and corporate data security governance requirements.

These tools provide the following features:

- 1. Data security categorization and classification:** BGs/BUs can create their own categorization and classification standards, and customize data levels and factors. This lays the groundwork for subsequent differentiated controls, thereby reducing data security risks and ensuring compliance.
- 2. Data inventory:** BGs/BUs can record the basic information, responsible parties, security status, and processing information of important and core data throughout the data lifecycle. They can also promptly update these records to maintain the latest status of the important data inventory online and review the accuracy and integrity of the inventory.
- 3. Data risk assessment management:** BGs/BUs can perform data security risk assessments for critical data processing activities based on the important data inventory. The assessments include compliance assessment, risk source identification, and security impact analysis. BGs/BUs can quantify risks using the preset risk impact matrix to draw comprehensive risk assessment conclusions.
- 4. Cross-border data transfer:** Scenarios involving cross-border transfers can be managed online and cross-border transfer agreements can be reviewed online. Regional or country-level subsidiaries can review cross-border transfer scenarios online to ensure the necessity, integrity, and accuracy of such data transfers.
- 5. One country, one policy:** Templates such as those for data inventories, processing records, and data transfer agreements (DTAs) can be tailored to meet different requirements set forth in the laws and regulations in different countries and regions, such as the Personal Information Protection Law of the People's Republic of China (PIPL), General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA).



04 Afterword

Data security is crucial for a thriving digital economy. It is a significant undertaking that requires a systemic approach. We will adopt a holistic approach to system development and foster alignment across all staff. And with a spirit of transformative determination, we will continue to enhance our data security governance capabilities and effectively integrate data security into our systems, processes, and business practices. This includes:

1. Firmly integrating data security capabilities throughout the product lifecycle, embedding data security into every phase of product development and service delivery, and ensuring that all products, solutions, and services come with inherent data security features.
2. Raise data security awareness and improve data security capabilities. Data security demands a robust defense. Every organization and individual plays a crucial role in this defense. We must leverage professional organizations and personnel, business processes, and efficient IT tools to enforce controls within the data security governance framework and achieve our security and compliance goals.

We remain committed to an open and collaborative approach to learning, working closely with industry partners to explore best practices in data security governance. We will continue to optimize the data security governance framework to ensure that business data is effectively protected and lawfully used and continue to improve the long-term mechanism for data security governance.



05 Appendix: Outline of Huawei's Data Security Governance Framework

L1 (Mainline)	L2 (Control Domain)	L3 (Control Item)
1. Data security governance	1.1 Strategy and policy	1.1.1 Strategic insight and regular review
		1.1.2 Policy and management system
	1.2 Requirements for organizations, processes, and capabilities	1.2.1 Organization
		1.2.2 Process
		1.2.3 Overall capability requirements
	1.3 Awareness and culture	1.3.1 All-staff training and awareness improvement
		1.3.2 Professional capability improvement
	1.4 Measurement and improvement	1.4.1 Measurement
		1.4.2 Inspection
		1.4.3 Audit
	1.5 Communication and social responsibility	1.5.1 Communication
		1.5.2 Social responsibility and social supervision
1.6 Data security incident	1.6.1 Data security contingency plan and incident response	
2. Data security implementation	2.1 Data inventory	2.1.1 Data security categorization and classification
		2.1.2 Data processing records and data assets
	2.2 Data security risk assessment	2.2.1 Data security risk assessment
	2.3 Data security lifecycle	2.3.1 Data collection
		2.3.2 Data transmission
		2.3.3 Data storage
		2.3.4 Data use
		2.3.5 Data circulation and cross-border transfer
		2.3.6 Data disposal
	3.1 Development phase	3.1.1 Data security requirements
3.1.2 Data security categorization and classification		
3.1.3 Data security risk assessment		
3.1.4 Design specifications on security by default and transparency by default		
3.1.5 Process and tool assurance throughout the data security lifecycle		
3.2 Operations phase		3.2.1 Data security incident and vulnerability management
		3.2.2 Platform and tool assurance
		3.2.3 Infrastructure security

Note: Due to space limitations, L4 (specific controls) is omitted in the preceding table.

Table 5-1 Series of controls in Huawei's data security governance framework