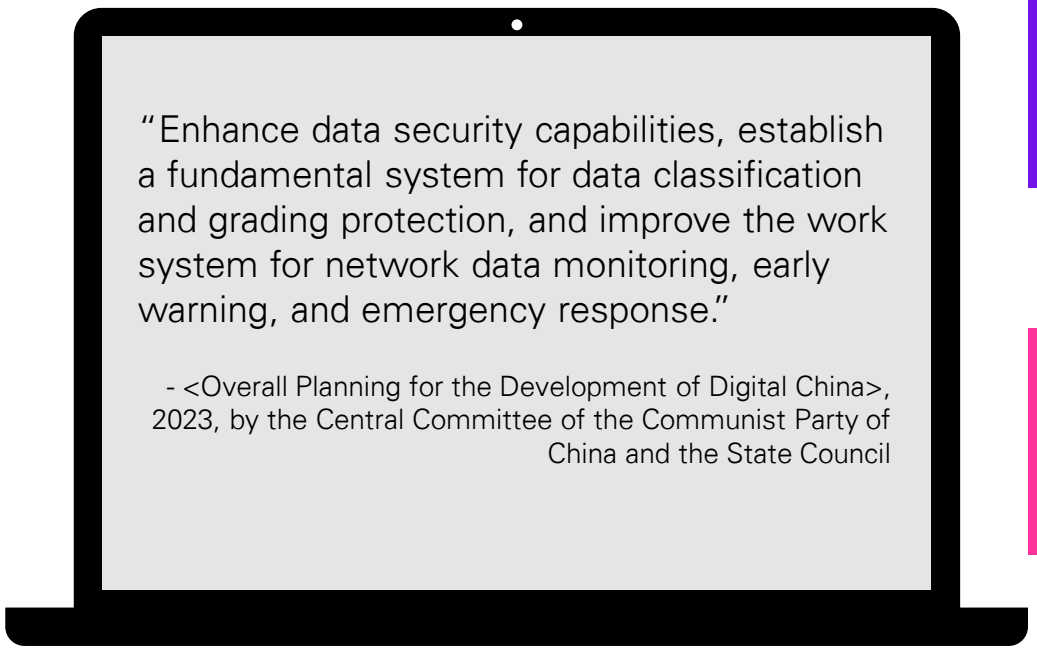
KPMG

Data security: Safeguarding High-quality Development of the Digital Economy

<Regulation for the Administration of Network Data Security> is finalised and will take effect January 1, 2025

November 2024

Enhancement of data security capabilities is a fundamental compliance obligation and a timely move to maintain competitiveness in the digital era



Enhancing data security capabilities is a fundamental compliance obligation

Data security management is undergoing a gradual shift from legislation to practice. Currently, the regulatory framework for personal information protection has become increasingly comprehensive, which has also promoted the standardization and systematization of data security management. The identification and protection of key data, as well as the exploration of flexible and convenient cross-border data regulatory mechanisms, are also continuously advancing. Businesses must remain vigilant and actively ensure compliance.

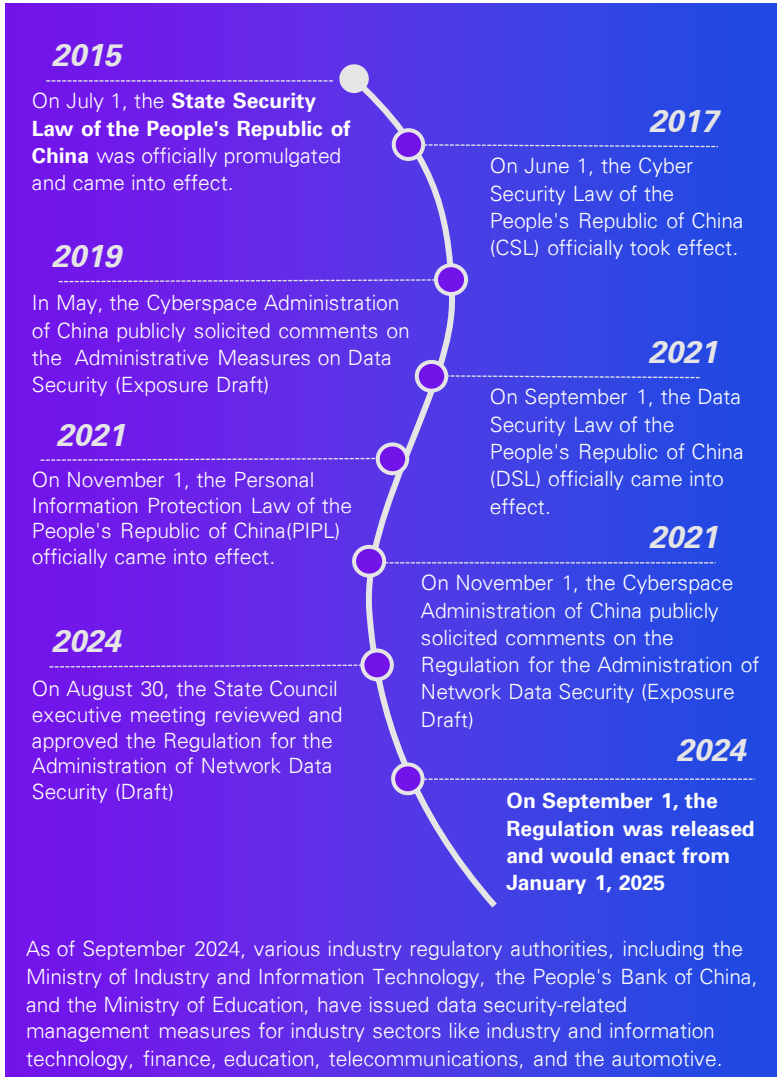
Data security is the driving force and foundation of technological innovation

As emerging technologies such as big data, artificial intelligence, and blockchain become more widely used, enterprises are facing new security challenges. To maintain seamless technological innovation, it is crucial for enterprises to continuously upgrade their security measures, paying close attention to data security, to identify and respond to potential risks.

Protecting data is protecting core competitiveness

Data contains business secrets, customer information and market insights, etc. The security and confidentiality of these data are directly related to the business stability and market competitiveness of enterprises. Only by strengthening data security management and ensuring data integrity and availability, can enterprises be invincible in the fierce market competition and achieve sustainable development.

The Regulation for the Administration of Network Data Security (the Regulation) is the first regulation by the State Council under the China CSL, DSL and PIPL



Applicable scope

- Network data processing activities conducted online within China, as well as the supervision and management of network data security
- Personal information processing activities conducted outside the country but fall into scope defined under PIPL Article 3
- Network data processing activities conducted outside the country but damaging the national security of the People's Republic of China, public interests, or the legitimate rights and interests of citizens or organizations
- This regulation does not apply to data processing activities carried out by natural persons for personal or household affairs.

Key focus

General provisions

- Data Security Strategy and Governance
- Data Security Lifecycle Management
- Data Security Management Framework
- Data Security Technology and Operation

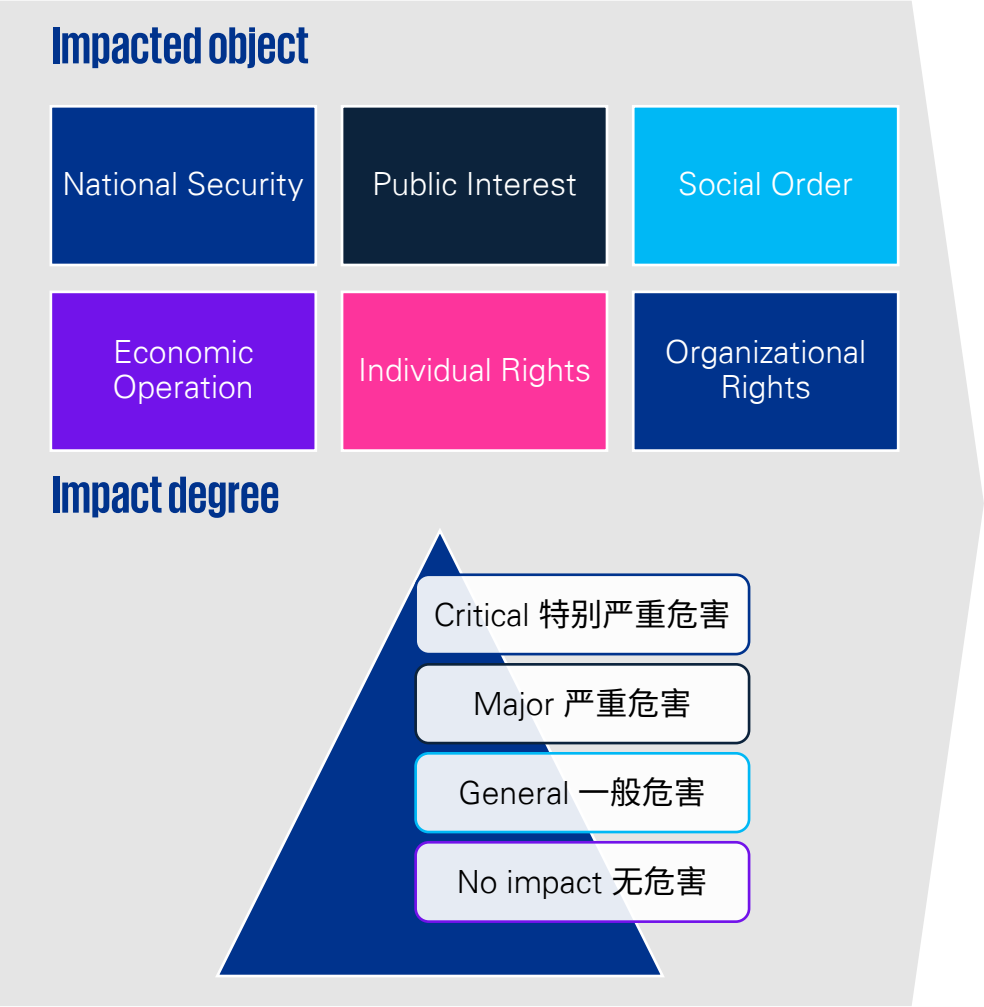
Special processing activities

- National security review
- Personal information protection
- Key data management
- Cross-border data transfer management
- Network platform service provider management

Consequences of non-compliance

- Generally refers to CSL, DSL and PIPL, with more details provided if violating requirements under general provisions, national security review or key data security management:
  - ❑ Fines (up to RMB 10 million for an organization; up to RMB 1 million for directly responsible supervisors and other responsible personnel)
  - ❑ Rectification, warnings, illegal gains confiscated, suspension for rectification, revoke of licenses etc.

Data security governance starts from Data Classification



According to the importance of data in economic and social development and the severity of harm caused by data leakage, tampering, destruction, or illegal access, use, or sharing, data is classified into three levels: core data, key data, and general data. General data is further graded into four levels (1 to 4) depending on the impacted object and impact degree.

Data Security Classification	Data Security Levels	Data Classification Criteria	
		Impacted object	Impact degree
General data	Level 1	Individual Rights, Organizational Rights	No impact
	Level 2	Individual Rights, Organizational Rights	General
	Level 3	Individual Rights, Organizational Rights	Major
	Level 4	Individual Rights, Organizational Rights	Critical
		Economic Operation, Social Order, Public Interest	General
Key data		Economic Operation, Social Order, Public Interest	Major
		National Security	General
Core data		Economic Operation, Social Order, Public Interest	Critical
		National Security	Critical or Major

References: GB/T 43697-2024 Data Security Technology – Rules for data classification and grading.

Focus of financial industry on data security governance

A series of industrial regulations and standards have been drafted and released for data security in the financial industry, including Administrative Measures of the People's Bank of China for Data Security in Business Fields (Exposure Draft), Administrative Measures for Data Security of Banking and Insurance Institutions (Public Exposure Draft), JR/T 0197-2020 Financial Data Security Guides of Data Security Classification, and JR/T 0171-2020 Personal Financial Information Protection Technical Specification. Once the Regulations on Network Data Security Management come into force, the financial industry should, in accordance with the relevant regulations and standards that have been released, focus on the following areas.

Data Classification and Categorization

- Sort out data assets according to business classification, identify important data and core data, and compile an important data directory
- Establish the implementation policies for data classification and categorization
- Take differentiated security protection measures according to data classification and categorization
- Implement dynamic management and maintenance of data directory

Administrative Measures for Data Security of Banking and Insurance Institutions (Public Exposure Draft)		Administrative Measures of the People's Bank of China for Data Security in Business Fields (Exposure Draft)
General data	Other general data	General data
	Sensitive data	
Important data		Important data
Core data		Core data

Key Challenges

- Consider the mapping relationship between data security levels for different regulations. Foreign banks should also consider domestic and overseas data assets as a whole to reduce management costs
- Inaccurate data classification will affect the implementation of differentiated security protection measures
- Dynamic management and maintenance is continuous rather than one-time work

Data Security Governance and Management

Security governance framework:

- Clarify the division of responsibilities of internal departments related to data security management, and refine the accountability procedures
- Designate a data security management department
- The important data processor shall specify in writing the person in charge of data security and the internal department responsible for data security leading management

Follow the basic principle of "who manages business, who manages business data, who manages data security"

Focus of financial industry on data security governance (cont'd)

Data Security Governance and Management

Construction of data security system:

- Establish relevant system requirements for data security governance, data classification and categorization, data security management, data security technology, data security risk monitoring, etc
- Data must be classified and managed accordingly; network data processors are responsible for the security of the data they handle

Data service management system:

- Establish a data service management system, formulate data service specifications, and establish a full-time data service team

Data Lifecycle Management

- In combination with JR/T 0197-2020 Financial Data Security Guides of Data Security Classification and JR/T 0223-2023 Specification for Security of Financial Data Security Data Life Cycle, the data security protection management requirements at different levels in all steps of data lifecycle are defined
- Implement the requirements of data security technical measures at different levels in all steps of the data lifecycle, including data collection, data processing, data usage, data sharing, entrusted processing, joint processing, data transfer and provision, data disclosure, data cross-border, data destruction and deletion, data transmission and data backup and storage
- Internal data sharing within the group should take protective measures, and sharing sensitive and confidential data should obtain authorization and consent from the data subject

Data Security Incident Management

- Establish a security risk monitoring and warning mechanism for data processing activities
- Formulate criteria and emergency plans for rating data security incidents
- Strengthen internal personnel and training management, strengthen personnel security awareness and implement emergency plans for security incidents
- Standardize emergency response and disposal according to different regulatory authorities and report incidents and disposal in a timely and orderly manner
- Shall accept public supervision by establishing convenient channels for network data security complaints and reports, publicize information on complaint and report channels, and promptly accept and handle network data security complaints and reports

Data Security Supervision and Management

- Establish data security compliance requirements and specifications
- Carry out comprehensive data security audit according to the requirements of different regulatory authorities
- Carry out a comprehensive data security risk assessment once a year, and complete the reporting as required
- Network data processors shall cooperate with the relevant authorities in conducting lawful supervision and inspection of network data security

Key Challenges

- At present, there are differences in the current regulatory requirements between the two parties. Financial institutions should seek common ground while reserving differences, analyse specific issues on a case by case basis and avoid redundant construction

- Take different security measures according to different data levels and build a data security technology protection system that adapts to the new technology environment
- When building a security control mechanism that covers the whole date lifecycle, it is necessary to consider the core technical capabilities of data security required in combination with the actual data scenarios, such as encryption, data desensitization, digital watermarking, data leakage prevention, privacy computing, data automatic grading and compliance, etc., and also consider how to implement the corresponding technologies through technical tools and product platforms (data security applications)

- When facing data security incidents, it is necessary to be able to quickly identify, evaluate, respond and restore business
- From the perspective of financial regulatory authorities, how to effectively manage data security incidents, including how to conduct emergency disposal and regulatory reporting after the event is focused. Financial institutions should focus on developing emergency processes and drills

- Normalize data security assessment and audit work and continue communication with regulators

Requirements for special processing activities

Focus on the integration and supplement with other relevant compliance requirements and practices

National security review

When network data processors engage in data processing activities that affect or may affect national security, they must undergo a national security review in accordance with relevant state regulations.

Other references: NSL, CSL, DSL, Security Protection Regulations for Critical Information Infrastructure, Cybersecurity Review Measures, etc.

Personal information protection

The overall compliance requirements for personal information processors should be based on the Personal Information Protection Law and other relevant personal information protection regulations, standards and guidelines. The following supplemental requirements noted from the Regulation:

- Specify the detailed conditions for transferring personal information and the specific implementation of data retention
- Records of the data processing when providing personal information to other network data processors or entrusting them to process it should be retained for at least 3 years
- Network data processors who are processing personal information of more than 10 million individuals must also comply with the relevant requirements for key data processors, including appointing the data security officer and establishing data security management organization, and conducting risk assessment before providing, entrusting, or jointly processing personal information.

Other references: PIPL, CSL, GB/T 35273 Personal Information Security Specifications, etc.

National security review

The overall compliance requirements for cross-border data transfer should be based on the Cybersecurity Law, Personal Information Protection Law, Data Security Law, and other related latest regulations for cross-border data transfer. The following supplemental requirements noted from the Regulation:

- The state shall take measures to prevent and address cross-border security risks and threats related to network data. No individual or organization is allowed to provide programs, tools, or other means specifically designed to damage or bypass technical measures. Knowing that others are engaged in such activities, one must not provide them with technical support or assistance.

Other references: CSL, PIPL, DSL, Security Assessment Measures for Cross-border Data Transfer, Measures on the Standard Contract for Cross-border Data Transfer of Personal Information, Provisions on Promoting and Regulating Cross-border Data Transfer, etc.

Requirements for special processing activities (cont'd) – Network platform service provider management

Network platform service provider management

The management requirements for data security of network platform service providers are proposed in the Regulation for the first time, mainly include:

- Shall clearly define the network data security protection obligations of third-party product and service providers that access their platform, and urge these third-party providers to strengthen network data security management. In particular, network platform service providers that distribute applications must establish application verification rules and conduct network data security-related verifications.
- For information pushed to individuals through automated decision-making processes, personalized recommendations should be easy to turn off, and personal characteristic tags should be removable
- The state encourages network platform service providers to support users in using public services for national network identity authentication to register and verify real identity information

In addition, **large network platform service providers**:

- Shall publish an annual social responsibility report on personal information protection
- When providing network data across borders, requirements for cross-border data security management must be followed, and relevant technical and management measures must be improved to prevent cross-border security risks related to network data
- It is prohibited to use network data, algorithms, or platform rules to engage in improper network data processing activities that harm users' legitimate rights
- If it involves the processing of key data, the annual risk assessment should fully explain the security status of key business operations and the supply chain related to network data

"**network platform service provider**" offers services to a large number of users and operators within the platform, which may include: social media platforms that provide information publishing and interaction, online platforms that offer payment services, online platforms that provide audio-visual services, online platforms that offer application distribution services, and manufacturers of smart devices with pre-installed applications etc.

"**large network platform service provider**" refers to those platforms with more than 50 million registered users or more than 10 million monthly active users, with complex business categories, whose network data processing activities have significant impacts on national security, economic operations, and the livelihoods of the citizens.

Requirements for special processing activities (cont'd) – Key data management

Key data management

The Regulation set clear requirements for processors of key data in the following areas :

Data Security Strategy and Governance

- ✓ Data security officer and data security management organization should be clearly defined. The data security officer must possess professional knowledge in data security and relevant management experience, and should be a member of the management team of the network data processor, with the authority to report the network data security status directly to the relevant authorities
- ✓ In the event of mergers, divisions, dissolution, bankruptcy, or other similar situations, a report must be submitted to the relevant authorities at or above the provincial level
- ✓ An annual risk assessment of its network data processing activities should be conducted, and the risk assessment report must be submitted to the relevant authorities at or above the provincial level

Data Security Lifecycle Management

- ✓ Providing, entrusting the processing of, or jointly processing must comply with additional requirements (e.g. risk assessment, retaining records of processing activities for at least 3 years etc.)

Data Security Management Framework, Technology and Operation

- ✓ The state encourages the use of data tagging and labelling tools to enhance the security management

Currently, regarding the identification and protection of important data, some industry regulatory authorities have clarified their data classification details, defining the scope of important and general data in sectors such as industry, telecommunications, healthcare, and education. Additionally, certain free trade zones have issued detailed regulations and identification guidelines for important data, such as the "Administrative Measures on Negative List for Outbound Data Transfer from China (Beijing) Pilot Free Trade Zone (for Trial Implementation)" and the " Standards for Data Classification and Grading by Enterprises in China (Tianjin) Pilot Free Trade Zone "

For industries where the definition and identification rules for important data are not yet clear, the GB/T 43697-2024 Data Security Technology – Rules for Data Classification and Grading and the "Information Security Technology – Guidelines for Identifying Important Data(Draft for Comments)" can be referenced to guide the identification process.

- Industrial manufacturing
- Telecommunication
- Transportation
- Financial service
- Natural Resources
- Healthcare
- Education
- Technology

Industrial manufacturing

- Administrative Measures on Data Security in the Field of Industry and Information Technology (for Trial Implementation)
- Guidelines for Identification of Important Data in the Industrial Field (YD/T4981-2024)
- Several Provisions on Automotive Data Security Management (Trial)

Financial service

- Administrative Measures of the People's Bank of China for Data Security in Business Fields (Exposure draft)
- Administrative Measures for Data Security of Banking and Insurance Institutions (Exposure draft)
- Guidelines for Data Security Classification (JR/T 0197-2020)

Telecommunications

- Guidelines for Identification of Key Data in the Telecommunications Sector (YD/T3867-2024)

Healthcare

- Guidelines for Data Classification in the Healthcare Industry (Trial)

Education

- Guidelines for the Identification of Core Data and Key Data in the Education System (Trial)

Recommended actions

> “Implement classified protection on network data, clearly define the responsibilities of various parties, and enforce network data security measures. It is essential to clarify security boundaries to ensure that data flows legally, orderly, and freely, thereby creating a favourable environment for promoting high-quality development of the digital economy and driving technological and industrial innovation.”

Optimize and implement data security classification

Further promote the effective implementation of data security classification, integrating compliance requirements with internal needs. Achieve a seamless connection between data asset classification and data security levels. Utilize technology and tools to enable data security classification, and to expand its coverage on data processing activities and system applications, laying a solid foundation for data lifecycle protection.

Establish and enhance data security governance

Promptly establish and improve the data security governance, including but not limited to data security protection principles, data lifecycle security management principles, data security incident management and emergency plans, data security complaint handling mechanisms, and data security risk and compliance management mechanisms.

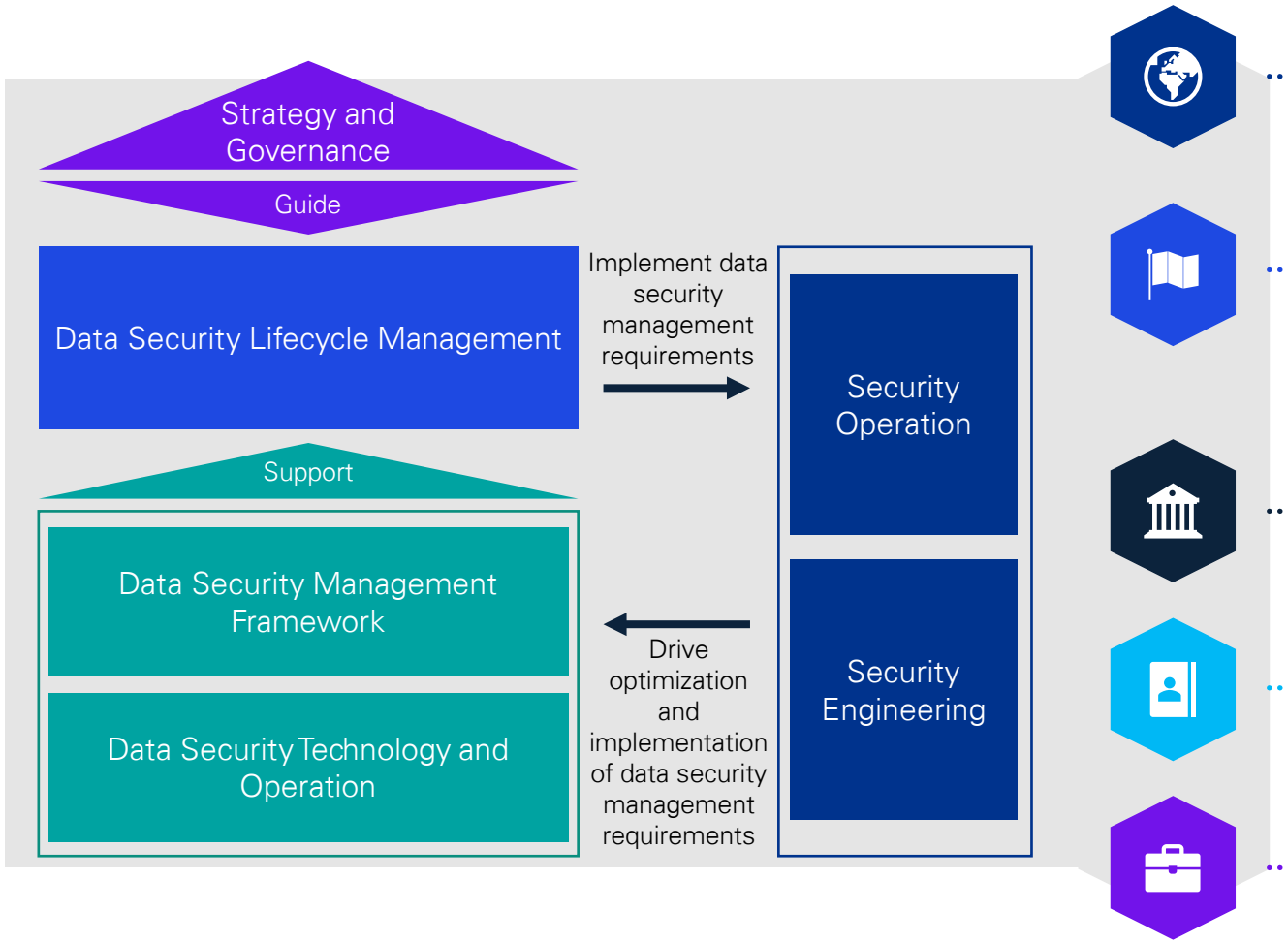
Improve data security management framework and technology with prioritization

For data with higher security level and its associated system platforms and infrastructures, to prioritize the implementation of data security management measures, including but not limited to, strengthening encryption controls, access controls, backup and recovery management mechanisms, and log and event monitoring mechanisms to effectively safeguard the integrity, confidentiality, and availability of such data.

Consider integration with privacy and security operation activities

Personal information, being a special type of data, requires specific management practices. The internal data security management organization and personnel should effectively integrate with the existing personal information protection framework. Additionally, data security measures should be aligned with traditional information and cyber security practices. Consider revisiting and adjusting current cyber security measures to ensure comprehensive data security.

KPMG provides one-stop solutions for managing data security risks



Data security classification design and implementation

Data security classification standards and tools design, data security classification management process design and implementation, and data security classification implementation etc.

Data security management governance planning and implementation

Data security management maturity assessment, data security management enhancement plan, data security management system design and implementation, cross-border data transfer compliance management etc.

Data security risk assessment / special review

Regular data security risk assessment, data security special audit for high-risk systems such as data warehouse/data lake/data management platform etc.

Data security incident response management

Emergency response plan, training, and drill etc.

Data leakage prevention management

Data leakage prevention requirement analysis, tool/vendor selection, technical implementation support and project management etc.

Contact Us

Richard Zhang
Partner
Technology Consulting
KPMG China
Tel: +86 (21) 2212 3637
Mail: richard.zhang@kpmg.com

Danny Hao
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (10) 8508 5498
Mail: danny.hao@kpmg.com

Quin Huang
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (21) 2212 2355
Mail: quin.huang@kpmg.com

Kevin Zhou
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (21) 2212 3149
Mail: kevin.wt.zhou@kpmg.com

Brian Cheung
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +852 2847 5062
Mail: brian.cheung@kpmg.com

Lanis Lam
Partner
Tech Risk, Technology Consulting
KPMG China
Tel: +852 2143 8803
Mail: lanis.lam@kpmg.com

Frank Wu
Director
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (21) 2212 3180
Mail: fm.wu@kpmg.com

Jason Song
Director
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (21) 2212 2888
Mail: jason.song@kpmg.com

Jason Li
Director
Tech Risk, Technology Consulting
KPMG China
Tel: +86 (10) 8508 5397
Mail: jz.li@kpmg.com

kpmg.com/cn/socialmedia

For more detail about KPMG China please scan the QR code or visit：https://home.kpmg/cn/zh/home/about/offices.html