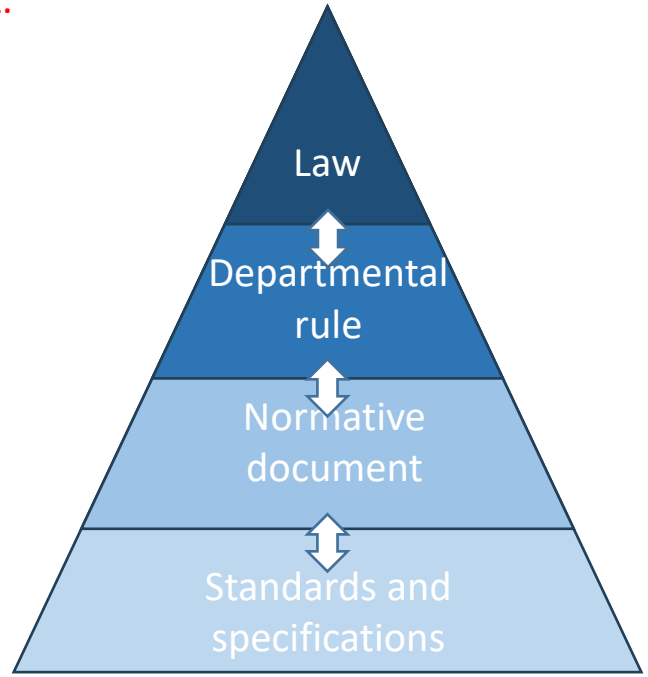
Overview of Standards for Cross-border Data Transfer

June 2024

Standards serve as a powerful tool for conducting data security work

As an important component of the national data security governance system, standards can provide specific support for laws, regulations, and policy documents, offer standard guidance for industrial practices and tackling difficult issues, and play a significant role in supporting laws and regulations, regulating product markets, serving key tasks, and guiding industrial development.



The ***Data Security Law*** proposes that "the nation shall promote the development and utilization of data technology and the construction of a data security standard system."

The ***Personal Information Protection Law*** stipulates that the state's cybersapce department shall coordinate with relevant departments to formulate specific rules and standards for the protection of personal information.

Twenty Data Measures and Overall Layout Plan for the Country's Digital Development

- deeply participate in the formulation of international high standard data rules, and explore and improve policies, standards, institutional mechanisms for data factor ownership, pricing, circulation, trading, usage, distribution, governance, and security.
- Construct a technical standard system, formulate guidelines for digital standardization work, and accelerate the formulation and revision of application standards for digital transformation across industries and integrated development of inter-industry convergence.

Introduction to SAC/TC 260

National Technical Committee 260 on Cybersecurity of Standardization Administration of China (SAC/TC260)

- Scope of work: standardization of cybersecurity technology, system, service, management, assessment, etc.
- Mirroring organization for ISO/IEC JTC1 SC27
- Working group: 9 working groups in total (see the figure on the right)
- Work to support the Data Security Law (DSL) and Personal Information Protection Law (PIPL):
  - DSL: 15 national standards published; 10 national standards under development;
  - PIPL: 17 national standards published; 9 national standards under development;
  - Coverage: security requirements, framkework and guidance, and testing and assessment.

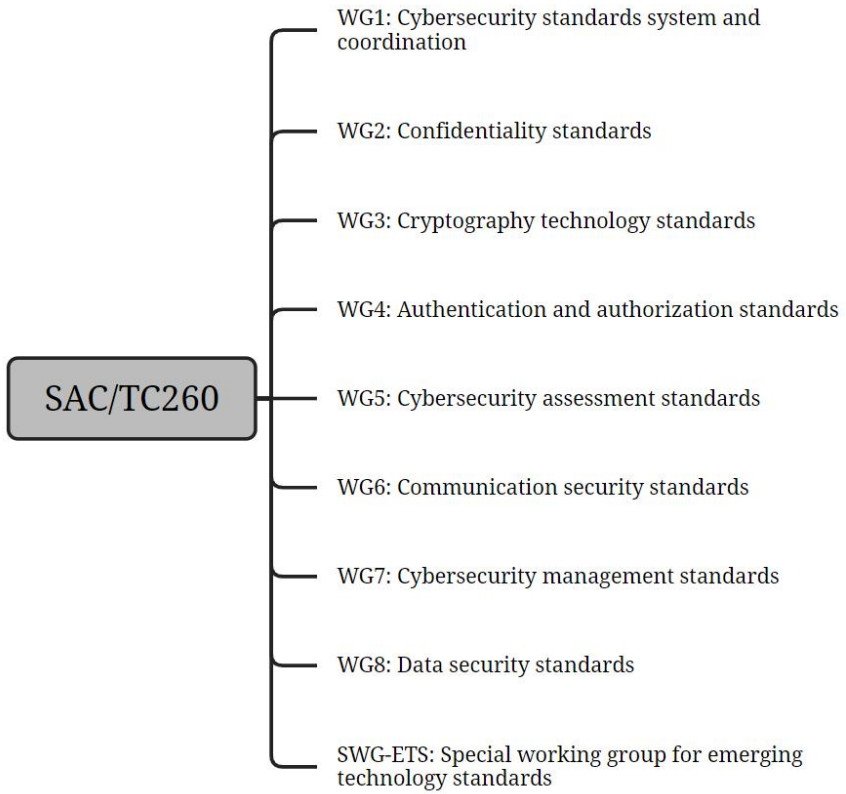


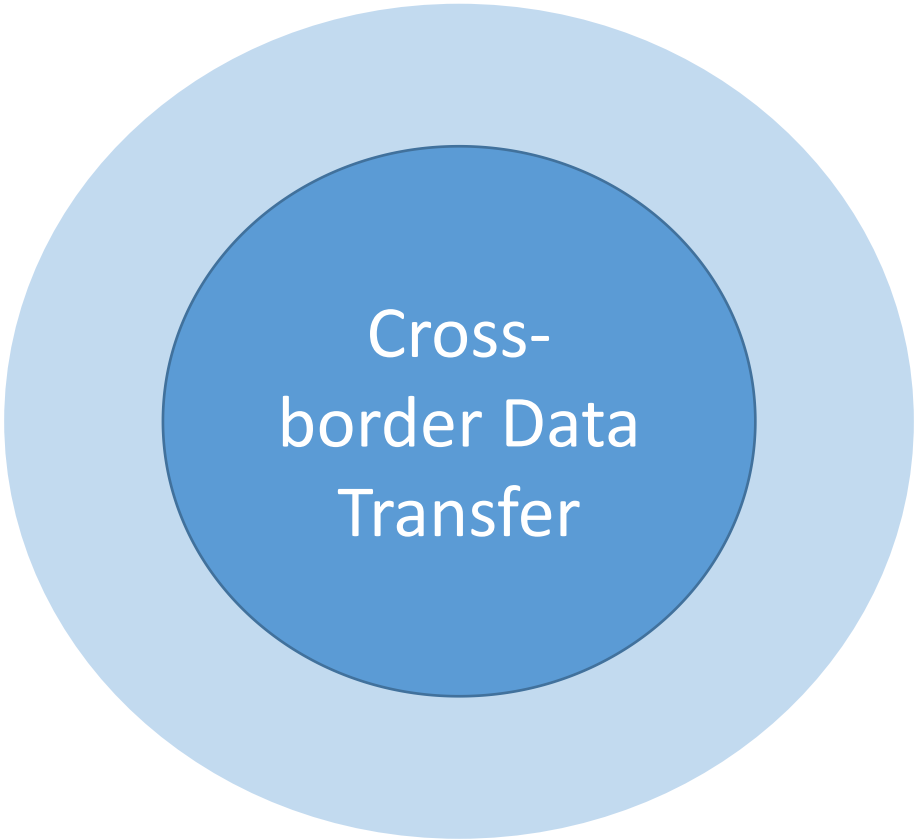
Figure 1. Working Groups of SAC/TC260

Data Cross-border Transfer Scenarios/Approach

1. Security Assessment

2. Personal Information Protection Certification

3. Standard Contract for Personal Information Cross-border Transfer

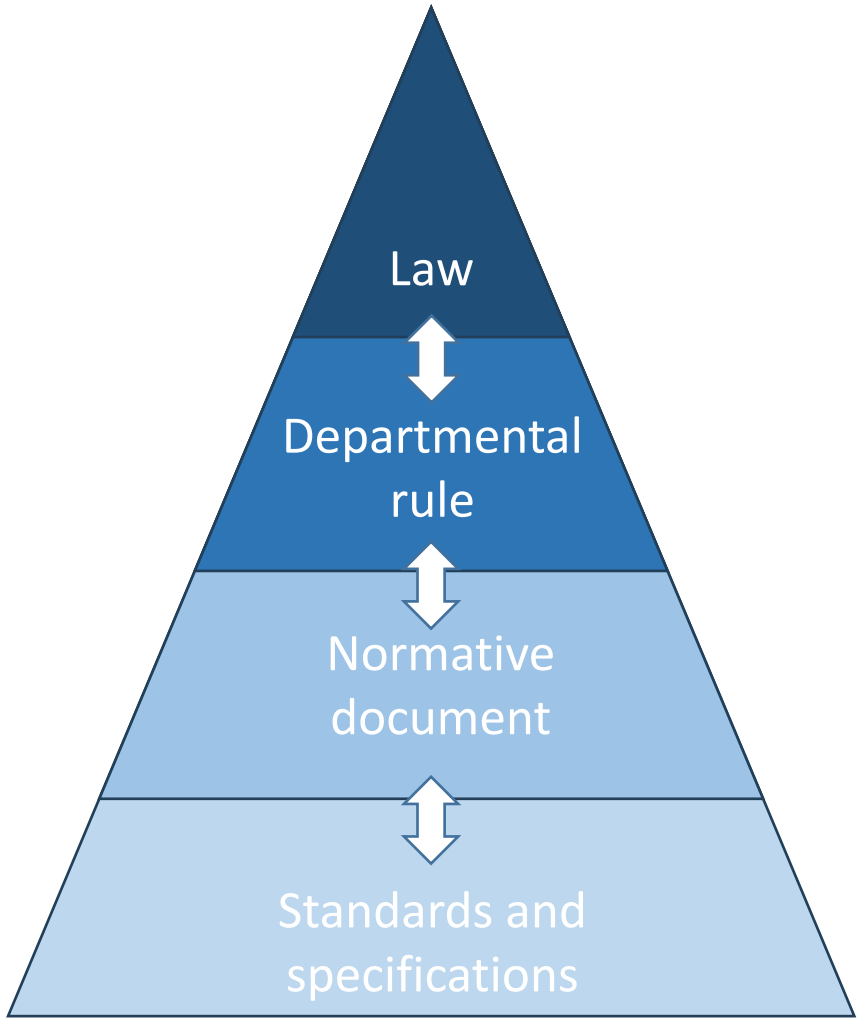


4. Exemption from Security Assessment, Certification and Standard Contract Signing

5. Cross-border Data transfer in Guangdong-Hongkong-Macao Greater Bay Area

6. Negative List in Free Trade Zone

Overview of Policies and Legislation for Cross-border Data Transfer



Laws:

- Cybersecurity Law
- Data Security Law
- Personal Information Protection Law

Departmental rules:

- Provisions on Promoting and Regulating Cross-border Data Flow
- Measures for the Security Assessment of Cross-border Data Transfer
- Measures for the Standard Contract for the Cross-border Transfer of Personal Information

Nomative documents:

- Announcement on the Implementation of Personal Information Protection Certification
- Guidelines for Application for Security Assessment of Cross-border Data Transfer (Second Edition)
- Guidelines for the Recordation of the Standard Contracts for the Cros-border Transfer of Personal Information (Second Edition)
- Implementation Guidelines on the Standard Contract for Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)

...

Standards and specifications:

GB/T 35273-2020 Personal information security specification
GB/T 43697-2024 Rules for data classification and grading
20230254-T-469 Security requirements for processing of sensitive personal information
GB/T 39335-2020 Guidance for personal information security impact assessment
20230255-T-469 Security certification requirements for cross-border processing activity of personal information
...

Major Standards for Cross-border Data Transfer

Requirement in legislation, departmental rules, and normative documents	Issues to be addressed by standards	Correspondent national standards
Provisions on Promoting and Regulating Cross-border Data Flow Scenarios that requires cross-border data transfer security assessment via cyberspace administration: • Critical Information Infrastructure Operator (CIIO) who transfers personal information or key data abroad • Non-CIIO that transfers key data abroad • Non-CIIO that transfers more than 1 million* non-sensitive personal information abroad (excluding sensitive information); • Non-CIIO that transfers more than 10, 000* sensitive personal information abroad	How to identify CII?	• GB/T 39204-2022 Cybersecurity requirements for critical information infrastructure protection • 20220603-T-469 Method of boundary identification for critical information infrastructure (draft for comment)
	How to identify key data?	• GB/T 43697-2024 Rules for data classification and grading
	How to identify personal information?	• GB/T 35273-2020 Personal information security specification • GB/T 43697-2024 Rules for data classification and grading
	How to identify sensitive personal information?	• 20230254-T-469 Security requirements for processing of sensitive personal information • Guidelines for Identifying Sensitive Personal Information

*Since January 1 of the current year, the cumulative amount of personal information provided overseas

Major Standards for Cross-border Data Transfer

Requirement in legislation, departmental rules, and normative documents

Measures for the Standard Contract for the Cross-border Transfer of Personal Information

Scenarios that requires recordation of standard contract:

- A personal information processor shall carry out a personal protection impact assessment before providing personal information abroad
- A personal information processor shall file the recordation to the local provincial cyberspace administration within 10 working days from the effective date of the standard contract. The following materials should be submitted for the record: standard contract and the personal information protection impact assessment report

Issues to be addressed by standards

How to conduct personal information protection assessment?

Correspondent national standards

GB/T 39335-2020 Guidance for personal information security impact assessment

Major Standards for Cross-border Data Transfer

Requirement in legislation, departmental rules, and normative documents	Issues to be addressed by standards	Correspondent national standards
Announcement on the Implementation of Personal Information Protection Certification Certification basis: • Compliance with *GB/T 35273 Personal information security specification* • For those transfer personal information abroad, compliance with *TC260-PG-20222A Security certification specification for cross-border processing of personal information* is also required.	Certification basis and correspondent standards	• *GB/T 35273 Personal information security specification* • *TC260-PG-20222A Security certification specification for cross-border processing of personal information* • • *20230255-T-469 Security certification requirements for cross-border processing activity of personal information (draft for approval)*
MOU on Promoting cross-border Data Flows in the Guangdong-Hong Kong-Macao Greater Bay Area: Personal information protection certification in Greater Bay Area	Certification basis and correspondent standards	• *TC260-PG-20222A Security certification specification for cross-border processing of personal information*

Major Standards for Cross-border Data Transfer

Requirement in legislation, departmental rules, and normative documents	Issues to be addressed by standards	Correspondent national standards
Personal information Protection Law: • Where a personal information processor provides personal information abroad, it shall inform the individual of the name or name of the overseas recipient, contact information, purpose of processing, method of processing, type of personal information and other matters such as the way and procedure for the individual to exercise the rights provided for in this Law with the overseas recipient, and obtain the individual's separate consent.	How to inform and obtain the individual's seperate consent?	• *GB/T 42574-2023 Implementation guidelines for notices and consent in personal information processing*
• *Guidelines for Application for Security Assessment of Cross-border Data Transfer (Second Edition):* Proof of the effectiveness of the processor's data security protection measures, such as data security risk assessment, data security certification, data security inspection and evaluation, data security compliance audit, and evaluation for classified protection of cybersecurity	How to carry out data security assessment and data security certification?	• *Measures for the Security Assessment of Cross-border Data Transfer, Implementation Guidelines for Data Security Risk Assessment* • *GB/T 37988 Data security capability maturity model (DSMM), Data Security Management Certification (DSM)* • *20240896-T-469 Personal Information Protection Compliance Audit Requirements*