Data Security Standards Application Framework and Capacity Enhancement Program

China Electronics Standardization Institute

2024/6/13

Data elements empower new quality productive forces

- **The construction of a basic data system is crucial to national development and security**. It is necessary to **safeguard national data security, protect personal information and commercial secrets**, promote the efficient circulation and utilization of data, and empower the economy. We must **coordinate and promote the efforts in fields of data ownership, circulation and trading, income distribution, and security governance, and accelerate the construction of a basic data system.**

It is necessary to highlight security throughout the entire process of data governance, uphold the security bottom line, clarify the regulatory red line, strengthen law enforcement and justice in key areas, and resolutely manage what must be paid attention to

Quote from the 26th Meeting of Central Commission for Comprehensively Deepening Reform

Opinions of the Central Committee of the CPC and the State Council on Building Basic Systems for Data to Give Full Play to the Role of Data Resources
(December 2022)

"Twenty Data Measures"

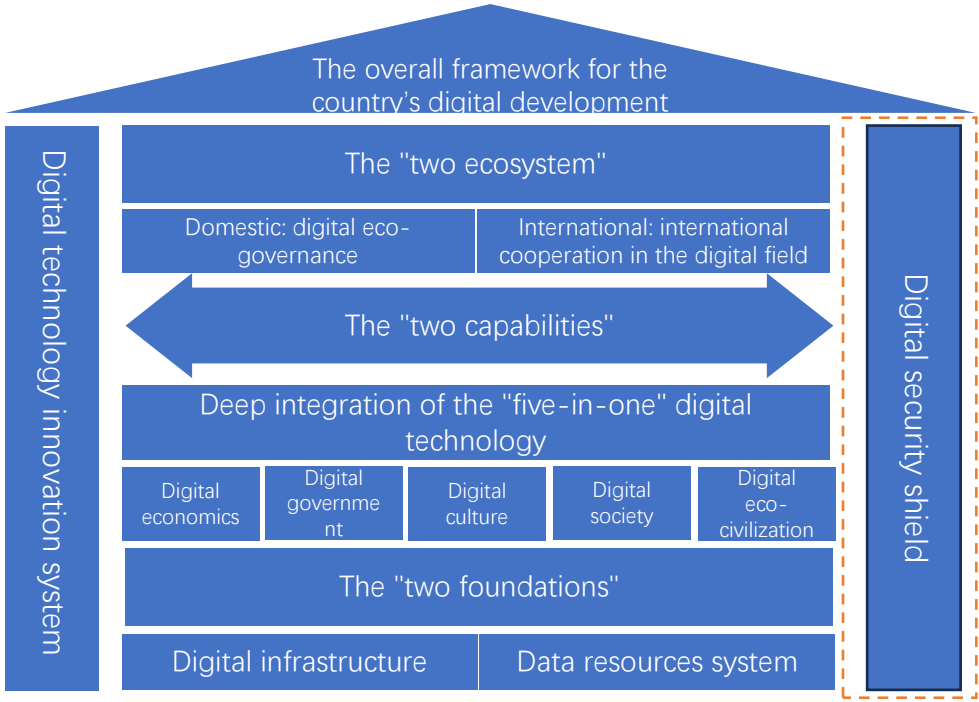
Series of Interpretations - General Requirements

Article 1: Guiding Principles

Guided by the Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, we should thoroughly implement the spirit of the 20th CPC National Congress, comprehensively and accurately carry out the new development philosophy, accelerate the construction of a new development paradigm, adhere to reform and innovation, and systematically plan and pursue.

The premise is to safeguard national data security, protect personal information and commercial secrets.	The key parts include data ownership, circulation and trading, income distribution, and security governance.
The mainline of the measures is to promote the efficient circulation and utilization of data, and empower economy.	The purpose is to extract value of data and share the benefits of economic development with all the people in this country.

In February 2023, the CPC Central Committee and the State Council issued the "**Overall Layout Plan for the Country's Digital Development**," points out the need to strengthen key capabilities for China's Dgital Development, establish an independent and innovative digital technology system, and **build a reliable and controllable digital security shield.**



The policies, regulations, and legal framework for data security have already been established

Highest legal effect.

The regulations, decisions, and ordinances issued by the State Council are subordinate to laws in terms of legal hierarchy and they needs to follow the requirement of relevant laws and provide support.

The documents issued by various departments of the State Council to guide daily work are more detailed in content compared to laws and regulations, and have the legal effect of administrative law.

Important principles

- Report to the 20th National Congress of the CPC
- The series of speeches by Xi Jinping on cyber security

Top-level design

- The Opinions of the CPC Central Committee and the State Council on Establishing a Better System and Mechanism for the Market-oriented Allocation of Factors of Production
- Internet Power Strategy
- National Cyberspace Security Strategy
- Opinions of the Central Committee of the CPC and the State Council on Building Basic Systems for Data to Give Full Play to the Role of Data Resources

Laws and regulations

- Cybersecurity Law
- Data Security Law
- Personal Information Protection Law
- Cryptography Law
- Civil Code
- Amendment to Criminal Law
- Consumer's Right and Interest Protection Law
- Decision on Strengthening the Information Protection on Network
- Network Data Security Management Regulations (Draft for Comment)
- Law on the Protection of Minors
- Regulations to Protect Minors in Cyberspace
- Regulation on Security Protection of Critical Information Infrastructure

Normative documents

- Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations
- Provisions on the Scope of Necessary Personal Information Required for Common Types of Mobile Internet Applications
- Announcement on Carrying Out the Certification Work for Data Security Management
- Announcement on the Implementation of Personal Information Protection Certification
- Ministry of Industry and Information Technology's nomative document [2019] No. 337, Ministry of Industry and Information Technology's nomative document [2020] No. 164...

Development plan

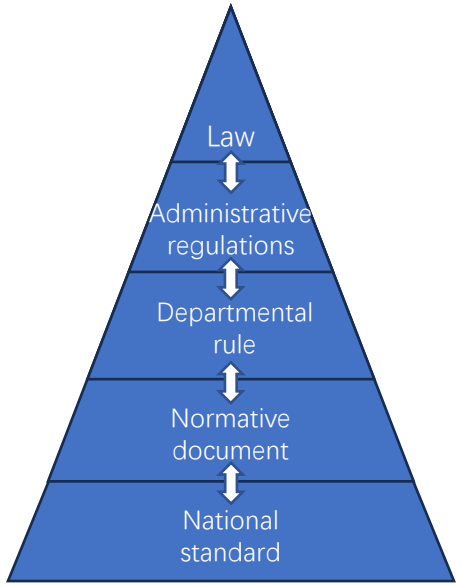
- The 14th Five-Year Plan of China
- The 14th Five-Year Plan for
- National Informatization
- Information Communication Network and Information Security Plan (2016-2020)
- The 14th Five-Year Plan for the Development of the Information and Communication Industry

Departmental rules

- Cybersecurity Review Measures of China
- Several Provisions on the Management of Automobile Data Security (for Trial Implementation)
- Provisions on Promoting and Regulating Cross-Border Data Flow
- The Measures for Security Assessment of Cross-border Data Transfer
- Provisions on the Cyber Protection of Children's Personal Information
- The Measures on the Administration of Data Security in the Field of Industry and Information Technology (Trial)
- Provisions on the Administration of Algorithm-generated Recommendation for Internet Information Services
- Interim Measures for the Administration of Generative Artificial Intelligence Services
- Standard Contract for the Cross-border Transfer of Personal Information
- Provisions on Protecting the Personal Information of Telecommunications and Internet Users
- Provisions on the Administration of Deep Synthesis of Internet-based Information Services

Since 2015, domestic data protection has been elevated to the level of legal norms, with laws and regulations gradually being completed. China has issued over **40** laws, regulations, and policy requirements, dedicated to data protection. They primarily cover **six major categories** of work requirements including **top-level design, legislation, administrative regulations, departmental rules, normative documents, and development plans.**

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.

- Uphold **coordinated development and security**
- Balance between data security and data utilization
- Insist on **promoting data security through data exploitation, utilization, and industrial development**, and **ensure data exploitation, utilization, and industrial development via data security**

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.

Research on reference framework for the standards application

- To promote the in-depth application of national standards for data security, **a reference framework for the application of data security and personal information protection standards** is proposed based on the principle of "prioritizing the foundation and gradually enhancing" and comprehensive consideration of factors such as the **supporting role of standards for laws and regulations, the scope of application of standards, the difficulty of implementation, and the level of security capabilities reflected.** The application of existing national standards for data security and personal information protection (including standard practice guidelines) is divided into three levels: basic application level, regular application level, and excellent application level.

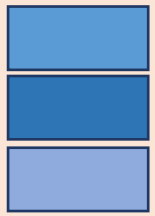
Research purpose	• Based on the statutory obligations stipulated in data security legislation, clearly define the baseline for data security compliance. • In order to addressing the practical needs of data security work, provide standardized data security solutions and pathways for capability enhancement. • Explore data security standards to safeguard data development, utilization, and industrial development, while promoting high-quality data supply, orderly data circulation, and compliant usage of data.

Research on reference framework for the standards application

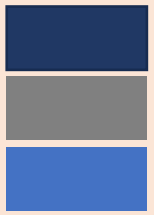
Basic Application Level	Pursuant to laws and regulations such as the *Data Security Law* and the *Personal Information Protection Law*, the statutory obligations of data processors are sorted out, and the standard documents **that directly support these obligations and reflect the baseline level of data security** are designated as the basic application level.
Regular Application Level	On the basis of the basic application level, the standard documents that **can be referenced to fulfill the defined obligations of the Data Security Law and reflect higher level of data security capabilities** are designated as the Regular application level.
Excellent Application Level	On the basis of the regular application level, standard documents **tailored for specific technologies or scenarios, with higher degree of implementation difficulty, or reflecting exceptional levels of data security capabilities**, are classified as the excellent application level.

Reference framework for data security standards

Distinguish general-purpose data processors from situation-based data processors



For general data processors



For situation-based data processors

Excellent Application Level

GB/T 37988-2019 Data security capability maturity model · lv.4	General Framework for the privacy computing	GB/T 39477-2020 Government information sharing—Data security technology requirements	Public data opening security requirements
GB/T 37973-2019 Big data security management guide	GB/T 39725-2020 Guide for health data security	GB/T 42447-2023 Data security guidelines for telecom field	Verification of Local Contour Processing Effect for Exterior Vehicle Scenes
Technical implementation guideline of digital watermarking	GB/T 42012-2022 Data security requirements for instant messaging services · excellent	GB/T 42014-2022 Data security requirements for online shopping services · excellent	GB/T 42016-2022 Data security requirements for online audio and video services · excellent
General framework for the confidential computing	GB/T 42013-2022 Data security requirements for express logistics services · excellent	GB/T 42015-2022 Data security requirements for internet payment services · excellent	GB/T 42017-2022 Data security requirements for online ride-hailing services · excellent

Regular Application Level

GB/T 37988-2019 Data security capability maturity model · lv.3	Technical method for risk monitoring of data application programming interface	Capacity requirements for assessment organization of data security	
GB/T 41479-2022 Network data processing security requirements	GB/T 42012-2022 Data security requirements for instant messaging services · regular	GB/T 42014-2022 Data security requirements for online shopping services· regular	GB/T 42016-2022 Data security requirements for online audio and video services · regular
GB/T 35274-2023 Security capability requirements for big data services	GB/T 42013-2022 Data security requirements for express logistics services · regular	GB/T 42015-2022 Data security requirements for internet payment services · regular	GB/T 42017-2022 Data security requirements for online ride-hailing services · regular

Basic Application Level

GB/T 43697-2024 Rules for data classification and grading	GB/T 41871-2022 Security requirements for processing of motor vehicle data	Security requirements for government data processing	
Requirements for data security protection	GB/T 37932-2019 Security requirements for data transaction service	Data security requirements for cloud computing services	
GB/T 37988-2019 Data security capability maturity model · lv.2	GB/T 42012-2022 Data security requirements for instant messaging services · basic	GB/T 42014-2022 Data security requirements for online shopping services · basic	GB/T 42016-2022 Data security requirements for online audio and video services · basic
Risk assessment approaches for data security	GB/T 42013-2022 Data security requirements for express logistics services · basic	GB/T 42015-2022 Data security requirements for internet payment services · basic	GB/T 42017-2022 Data security requirements for online ride-hailing services · basic

Reference framework for data security standards

Based on the current situation of enterprise data security practices, the contents of orange-circled standards are classified into three levels accordingly.

Excellent Application Level

Regular Application Level

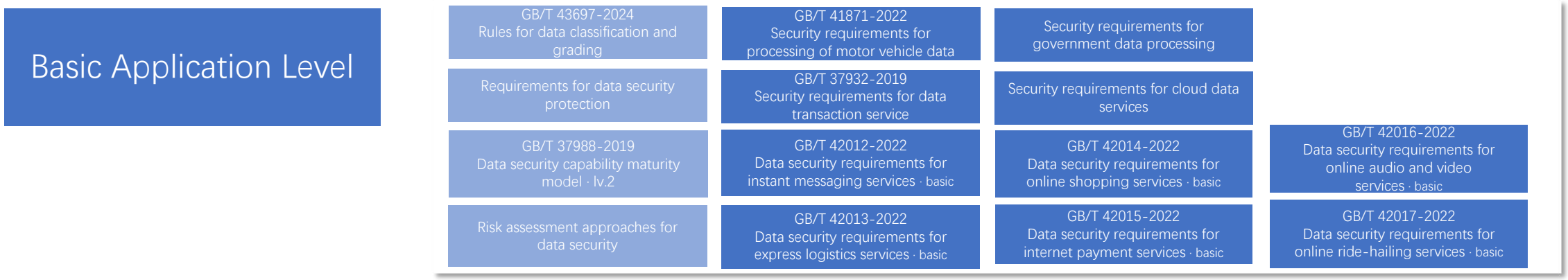
Basic Application Level

Example: application of data security standards for ride-hailing

GB/T 42017-2022 Information security technology - Data security requirements for online ride-hailing services

- **Basic application level**: 47 standard clauses, e.g.:
  - The passenger-side APP and the driver-side APP should not apply for any system permissions unrelated to their services. The scope of system permissions application and usage requirements are detailed in Annex D.
  - A virtual phone number should be used as communication channel for passengers and drivers.
- **Regular application level**: 58 standard clauses, e.g.:
  - When collecting travel tracks, the collection of location information through system location permissions should not exceed once per second.
- **Excellent application level**: 89 standard clauses, e.g.:
  - Watermark technology should be adopted for trip recordings to prevent the risk of leakkage such as audio transcription and video interception.

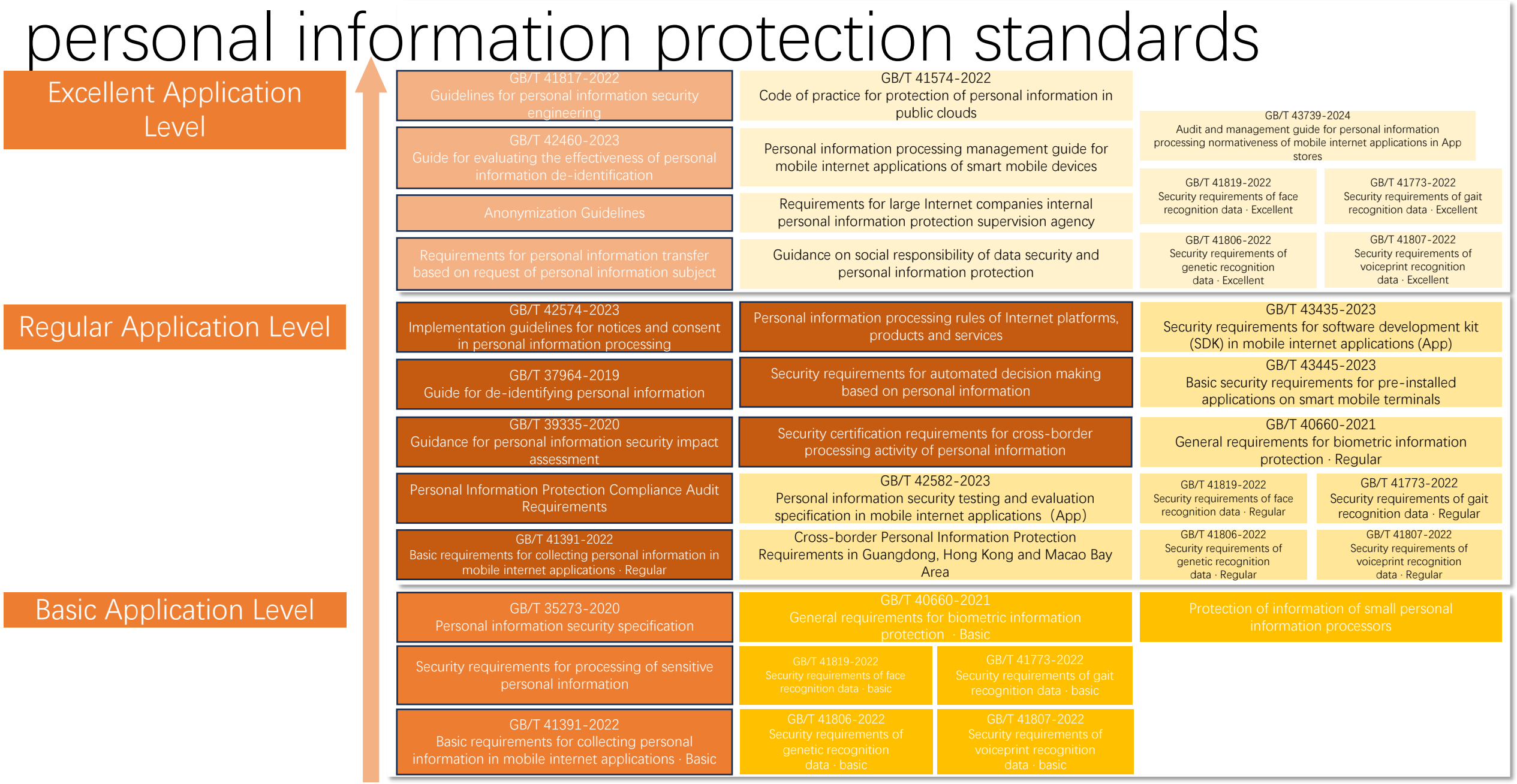
Reference framework for data security standards



Data Security Law 's requirements:

- Classified and graded data protection
- Emergency response to data security
- Monitoring of data security risks
- Data ethics
- Data access by national authorities
- Full-process data security governance
- Person in charge of data security and governance body
- Legitimate collection and use of data
- Approval of providing data to foreign judicial or law enforcement agencies
- Data cross-border security
- Data security risk assessment
- Data security education and training
- Administrative licenses for data processing services
- .....

Reference framework for the application of personal information protection standards



Reference framework for the application of personal information protection standards: basic level

Basic Application Level

GB/T 35273-2020 Personal information security specification	GB/T 40660-2021 General requirements for biometric information protection · Basic		Protection of information of small personal information processors
Security requirements for processing of sensitive personal information	GB/T 41819-2022 Security requirements of face recognition data · basic	GB/T 41773-2022 Security requirements of gait recognition data · basic	
GB/T 41391-2022 Basic requirements for collecting personal information in mobile internet applications · Basic	GB/T 41806-2022 Security requirements of genetic recognition data · basic	GB/T 41807-2022 Security requirements of voiceprint recognition data · basic	

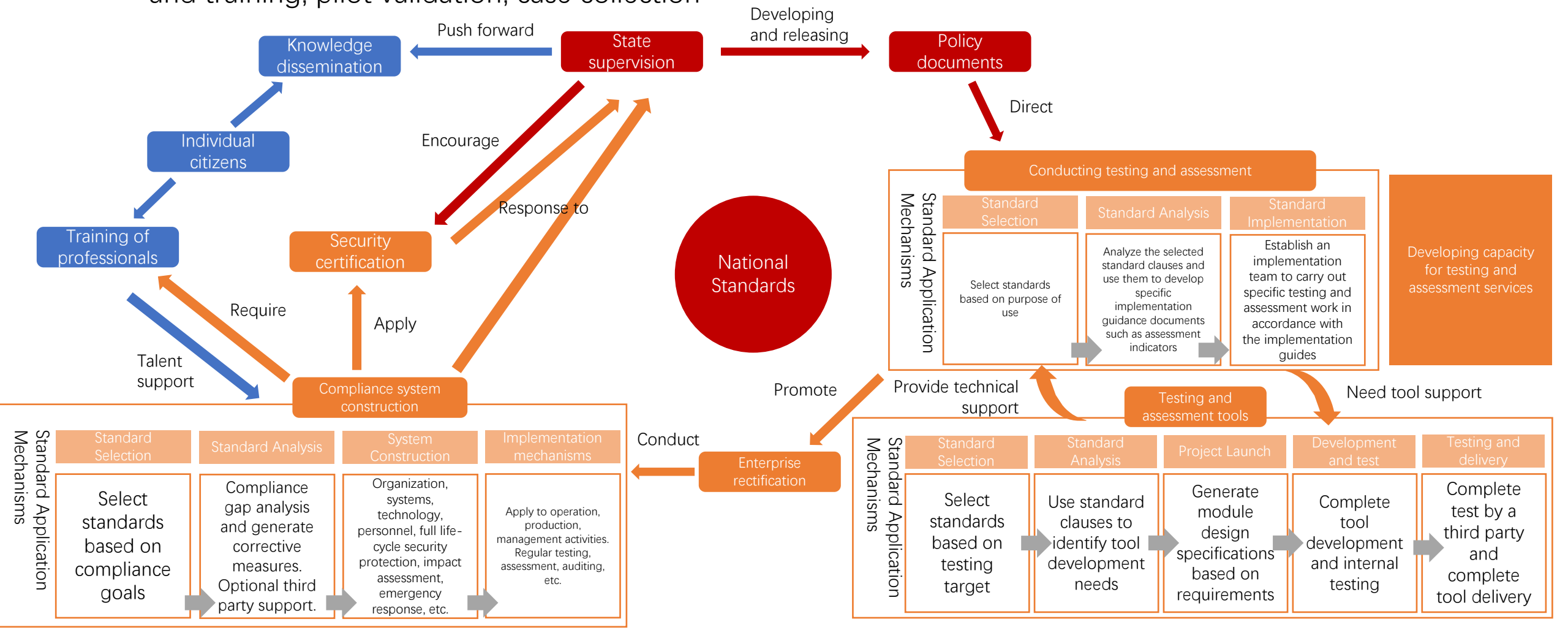
Personal Information Protection Law's requirements:

- Personal information processing principles
- Notices and consent in personal information processing
- Protection of minors' personal information
- Emergency response to personal information security incident
- Personal information protection impact assessment
- Personal information protection compliance audit
- Designated person in charge of personal information protection
- Personal information technical measures
- Categorized management of personal information
- Cross-border transfer of personal information
- Rights protection of subjects of personal information
- Requirements on large online platforms

...

Establish a mechanism for the application and promotion of integrated standards

- Policy support, standards development, technology development, testing and evaluation, publicizing and training, pilot validation, case collection……



Welcome to Join the Data Security Standards Enhancement Program (DSEP)

- Tel: 010-64102744
- E-mail: nispsslab@163.com
- Contacts:
- Yingjie Ren: 186 1381 8629
- Chao Gao: 186 1057 2925
- Chentao Gao: 131 4143 0192