WE WILL START AT 10:00 AM (CET)

SESEC Webinar 18: China’s Standardization in the Digital Sector: A Comprehensive Overview

You are ***muted***

Use the ***Q&A or Chat Panel*** to submit your questions

Keep your questions ***short and concise***

Contact us: assistant@sesec.eu

Welcome to our website: https://sesec.eu/

Seconded European Standardization Expert in China (SESEC) Project

SESEC INTRODUCTION

Partners and Role

SESEC Partners

SESEC is a visibility project co-financed by five European partners

- **European Commission (EC)**-The executive body of the European Union; Responsible for proposing legislation, implementing decisions, upholding the treaties and day-to-day management of the EU; DG Grow is the main partner (80%)
- **European Free Trade Association (EFTA)-**Iceland, Liechtenstein, Norway and Switzerland; Intergovernmental organisation set up for the promotion of free trade and economic integration to the benefit of its four Member States; None EU members;
- **CEN**-European Committee for Standardization
- **CENELEC**-European Committee for Electrotechnical Standardization
- **ETSI**-European Telecommunications Standards Institute

SESEC INTRODUCTION

A Project co-funded by EC, EFTA, CEN CENELEC & ETSI

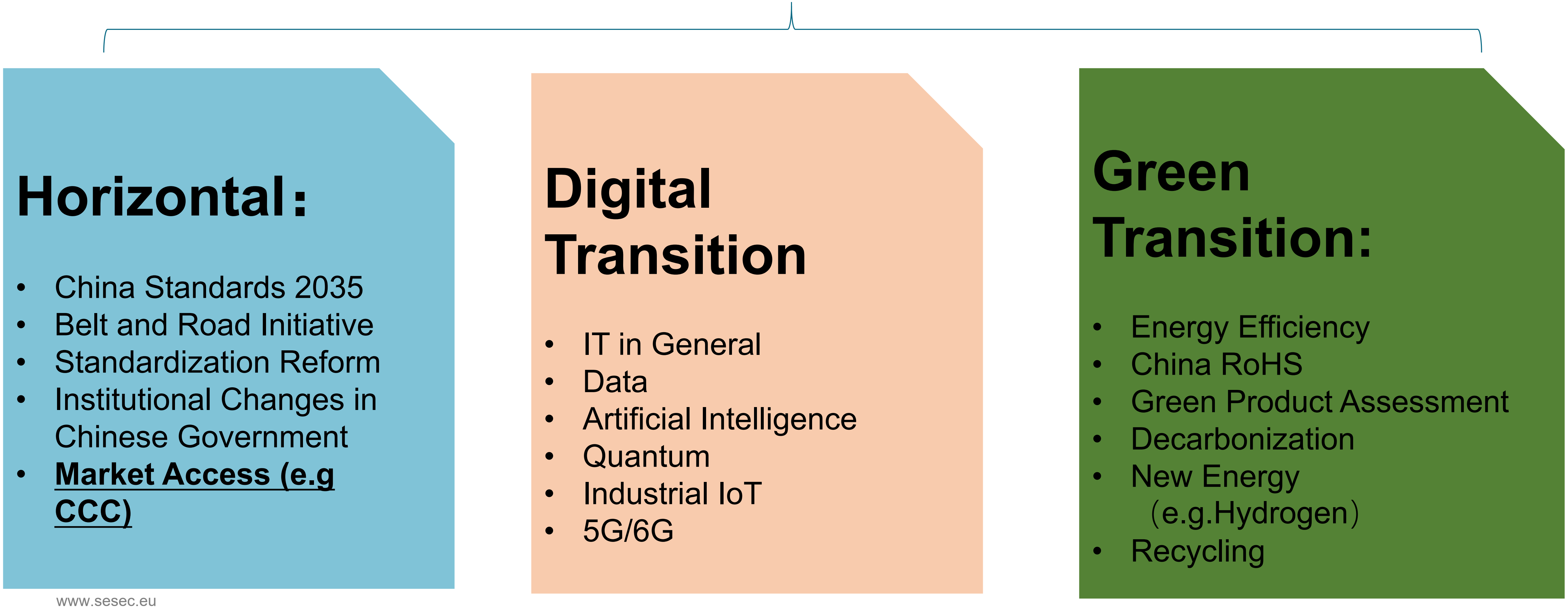
- ❖**Promote** European and International standards in China
- ❖**Improve** contacts between Project Partners and different levels of the Chinese administration, industry and standardization bodies
- ❖**Enhance** visibility and understanding of the European Standardization System (ESS) in China.
- ❖**Gather** regulatory and standardization intelligence
- ❖**Undertake** technical lobbying

Goals

- The SESEC initiative supports **EC policy** and **ESOs strategic objectives** in China.
- Our ultimate goal is the enhancement of **EU-China dialogue and cooperation** in the field of standardization.
- It is notably expected to support the Framework Cooperation Agreement in place **between the ESOs and SAC.**

Project’s Priorities

Priorities of SESEC



Horizontal:

- China Standards 2035
- Belt and Road Initiative
- Standardization Reform
- Institutional Changes in Chinese Government
- **Market Access (e.g CCC)**

Digital Transition

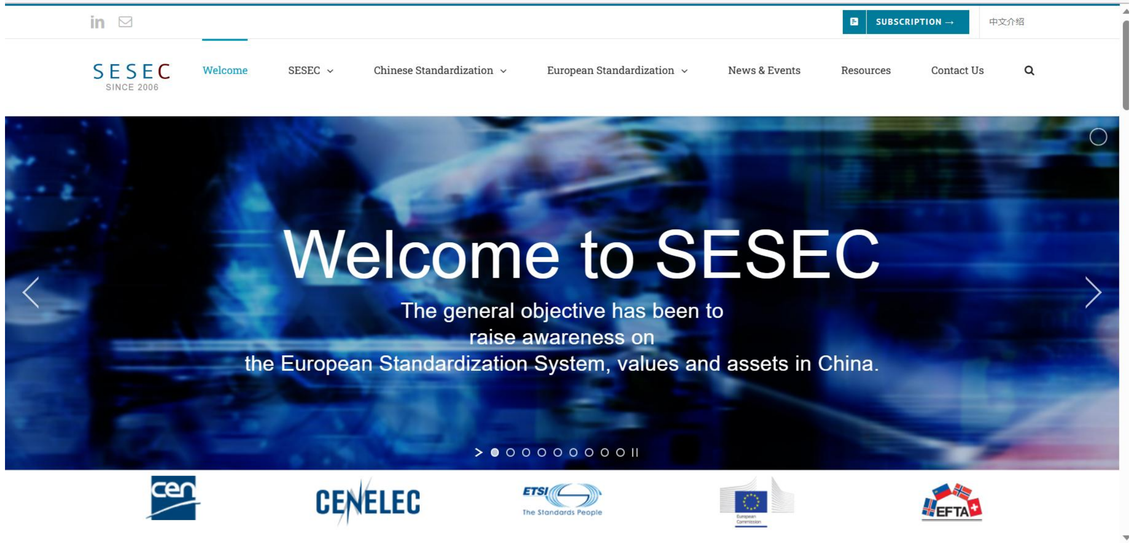
- IT in General
- Data
- Artificial Intelligence
- Quantum
- Industrial IoT
- 5G/6G

Green Transition:

- Energy Efficiency
- China RoHS
- Green Product Assessment
- Decarbonization
- New Energy （e.g.Hydrogen）
- Recycling

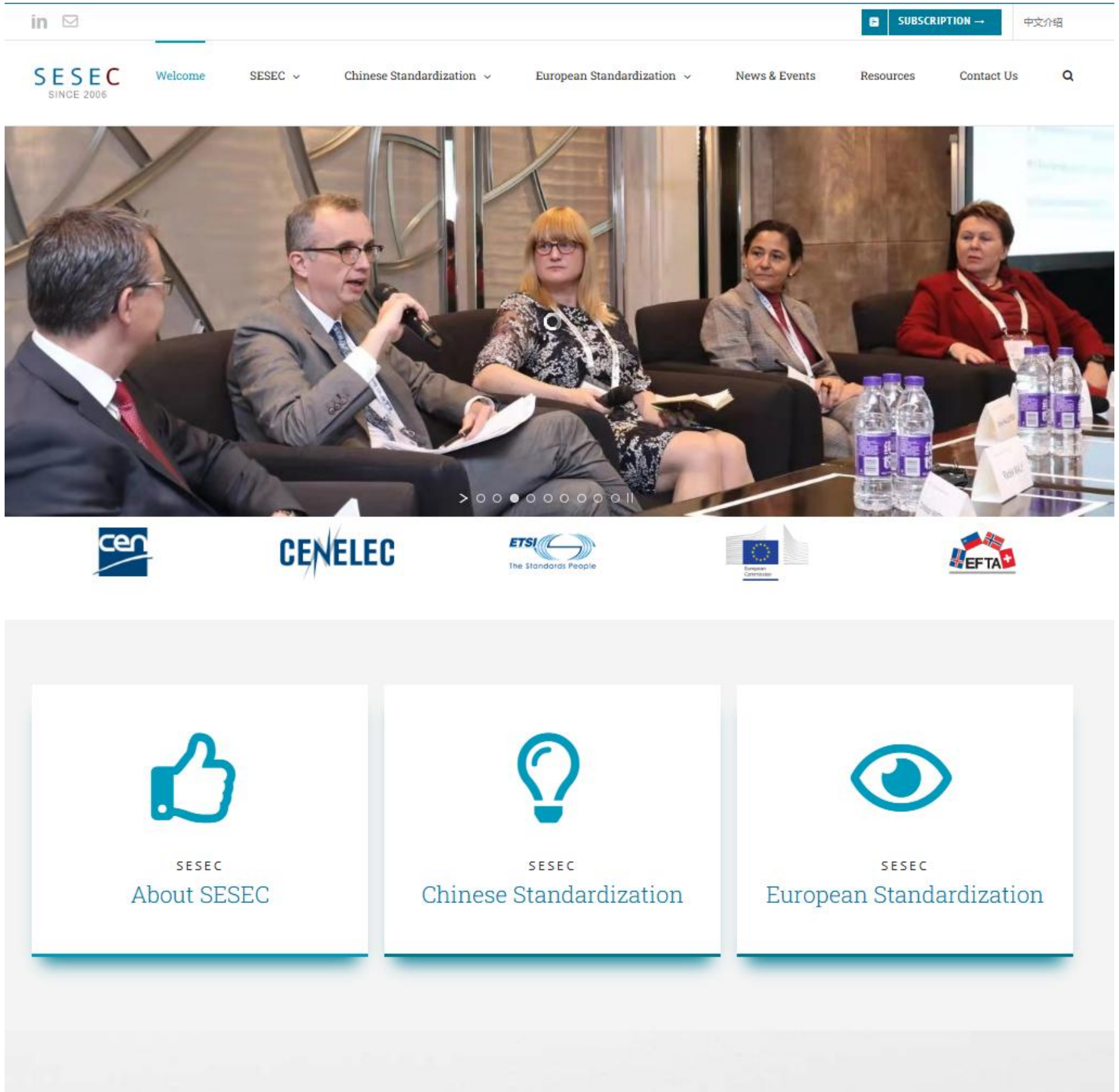
SESEC's English Website
For European stakeholders

www.sesec.eu



Welcome to SESEC

The general objective has been to
raise awareness on
the European Standardization System, values and assets in China.



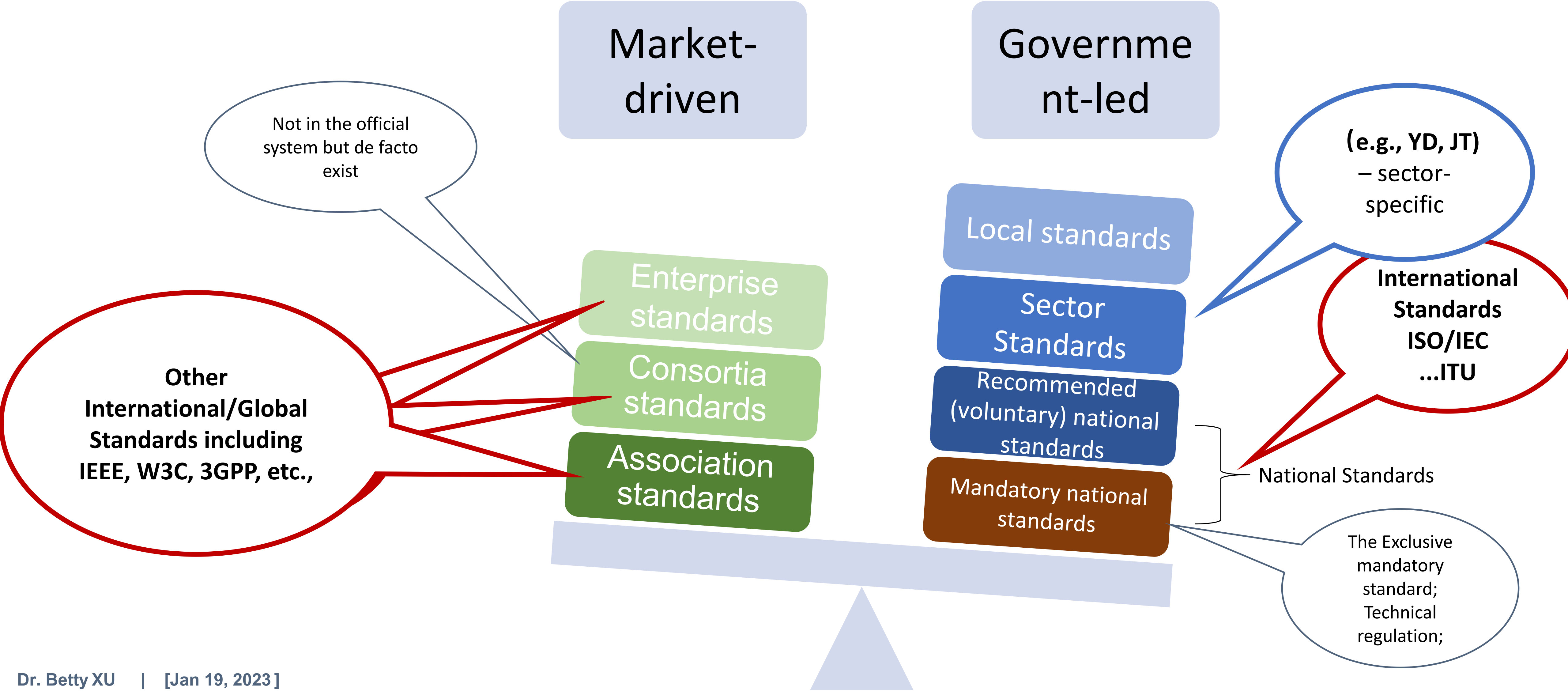
Chinese Standardization – Digital Sector as of Feb 2025

CONTENTS

1. Overview
2. AI
3. Cybersecurity
4. Data
5. Industry IoT /Smart Standards
6. Quantum
7. Summary

China Standardization System

5 levels – National Standards, Sector Standards, Local Standards, Association Standards, and Enterprises Standards


Market-driven
Government-led
Not in the official system but de facto exist
Enterprise standards
Consortia standards
Association standards
Other International/Global Standards including IEEE, W3C, 3GPP, etc.,
Local standards
Sector Standards
Recommended (voluntary) national standards
Mandatory national standards
(e.g., YD, JT) – sector-specific
International Standards ISO/IEC …ITU
National Standards
The Exclusive mandatory standard; Technical regulation;

Overview of China Digital Standardization
Key managing organizations

Agency	Role
SAC (Standardization Administration of China)	Coordinates national standard development
MIIT (Ministry of Industry and Information Technology)	Leads digital infrastructure and ICT-related standards
CAC (Cyberspace Administration of China)	Oversees standards related to cybersecurity and data governance
NDRC, MOST, NDA, MOT etc.	Involved in sectoral digital transformation efforts

CESI

1. The Electronics Standardization Institute (CESI) is a public institution directly under the MIIT， specializing in standardization research within the industrial and electronic information technology sectors
2. 45 Domestic technical mirrors of ISO、IEC、ISO/IEC JTC1
3. 17 Secretariat of the National Technical Committee for Standardization
4. Secretariat of the Sub-Technical 24 Committee of the National Standardization Technical Committee

CCSA

5G/5G-Advanced, 6G

- IPv6
- Quantum Communication
- intelligent connected vehicles
- AI
- Big Data
- Cloud Computing
- Block Chain
- VR
- IoT
- Fiber Communication

TCs Under other Institutions

02 China AI Standardization - **SAC/TC28/SC42**

Introduction of SAC/TC28/SC42 – Mirror ISO/IEC/JTC1/SC42

- **Full name:** National Artificial Intelligence Standardization Technical Committee
- **Year of establishment:** 2020
- **Secretariat unit:** CESI (China Electronics Standardization Institute)
- **Number of member organizations:** 488
- **Subordinated WGs:** 14 Working groups
- Supporting policies drafting of **MIIT** and **MOST**

Exisiting working groups:

1. Working Group of Fundamental Standards (international standards)
2. Research Group of Chips and Systems
3. Research Group of Model and Algorithm
4. Research Group of Products and Services
5. Research Group of Trustworthiness
6. Working Group of Computer Vision
7. Working Group of Knowledge Graph
8. Working Group of Automated Driving

Newly-established WGs in 2023/2024

1. WG of Humanoid Robot
2. WG of Opensource
3. WG of Intelligent Computing
4. WG of AI’s application in Electric Power Industr
5. WG of Smart Living
6. WG of AI Application in Medical Care

Proposed WGs to be established:

1. WG of AI for Science
2. WG of AI’s Application in Iron and Steel Industry
3. WG of AI’s Application in Energy
4. WG of AI’s Application in Railway Station
5. ...

AI in General - SAC/TC28/SC42 Aritifical Intelligence

Statistics

National standards:

- **15** published national standards
- **50+** national standards under development or to be officially established;

Sector standards:

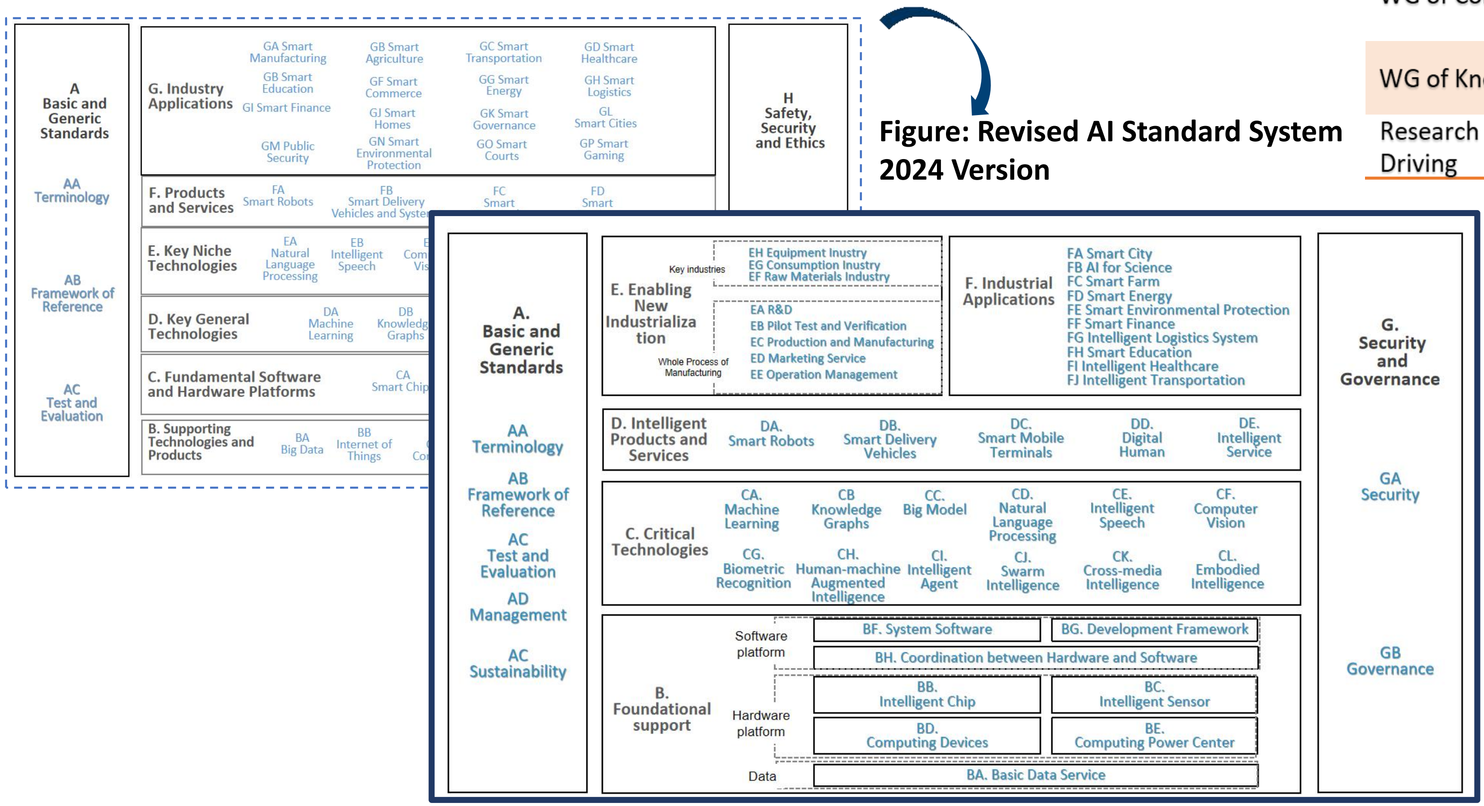
- **34** officially registered in areas of intelligent computing chip training, training data sets, industrial vision, and automated driving

International standards:

- Around **10** officially published ISO/IEC standards (including the international standards, technical report and technical specifications): ISO/IEC TR 24372, ISO/IEC TS 4213, ISO/IEC 5392, ISO/IEC 5259-4, ISO/IEC TS 8200

Table: Subordinated working groups of SAC/TC28/SC42

Name of WG	Newly-established in 2023	Newly-established in 2024
WG of Fundamental Standards	WG of Humanoid Robot	WG of AI's Application in Iron and Steel Industry
Research Group of Chips and Systems	WG of Opensource	WG of AI's Application in Logistics
Research Group of Models and Algorithms	WG of Intelligent Computing	WG of AI's Application in Communication
Research Group of Products and Services	WG of AI's application in Electric Power Industry	WG of AI's Application in Construction
Research Group of Trustworthiness	WG of Smart Life	WG of AI's Application in Finance
WG of Computer Vision	WG of AI's Application in Medical Care	WG of AI's Application in Mining
WG of Knowledge Graph		Research Group of AI Big Model Benchmarking
Research Group of Automated Driving		



A Basic and Generic Standards: AA Terminology; AB Framework of Reference; AC Test and Evaluation

G. Industry Applications: GA Smart Manufacturing; GB Smart Agriculture; GC Smart Transportation; GD Smart Healthcare; GB Smart Education; GF Smart Commerce; GG Smart Energy; GH Smart Logistics; GI Smart Finance; GJ Smart Homes; GK Smart Governance; GL Smart Cities; GM Public Security; GN Smart Environmental Protection; GO Smart Courts; GP Smart Gaming

F. Products and Services: FA Smart Robots; FB Smart Delivery Vehicles and Syster; FC Smart; FD Smart

E. Key Niche Technologies: EA Natural Language Processing; EB Intelligent Speech; E Com Vis

D. Key General Technologies: DA Machine Learning; DB Knowledg Graphs

C. Fundamental Software and Hardware Platforms: CA Smart Chip

B. Supporting Technologies and Products: BA Big Data; BB Internet of Things; C Co

H Safety, Security and Ethics

Figure: Revised AI Standard System 2024 Version

A. Basic and Generic Standards: AA Terminology; AB Framework of Reference; AC Test and Evaluation; AD Management; AC Sustainability

E. Enabling New Industrialization
Key industries: EH Equipment Inustry; EG Consumption Inustry; EF Raw Materials Industry
Whole Process of Manufacturing: EA R&D; EB Pilot Test and Verification; EC Production and Manufacturing; ED Marketing Service; EE Operation Management

F. Industrial Applications: FA Smart City; FB AI for Science; FC Smart Farm; FD Smart Energy; FE Smart Environmental Protection; FF Smart Finance; FG Intelligent Logistics System; FH Smart Education; FI Intelligent Healthcare; FJ Intelligent Transportation

D. Intelligent Products and Services: DA. Smart Robots; DB. Smart Delivery Vehicles; DC. Smart Mobile Terminals; DD. Digital Human; DE. Intelligent Service

C. Critical Technologies: CA. Machine Learning; CB Knowledge Graphs; CC. Big Model; CD. Natural Language Processing; CE. Intelligent Speech; CF. Computer Vision; CG. Biometric Recognition; CH. Human-machine Augmented Intelligence; CI. Intelligent Agent; CJ. Swarm Intelligence; CK. Cross-media Intelligence; CL. Embodied Intelligence

B. Foundational support
Software platform: BF. System Software; BG. Development Framework; BH. Coordination between Hardware and Software
Hardware platform: BB. Intelligent Chip; BC. Intelligent Sensor; BD. Computing Devices; BE. Computing Power Center
Data: BA. Basic Data Service

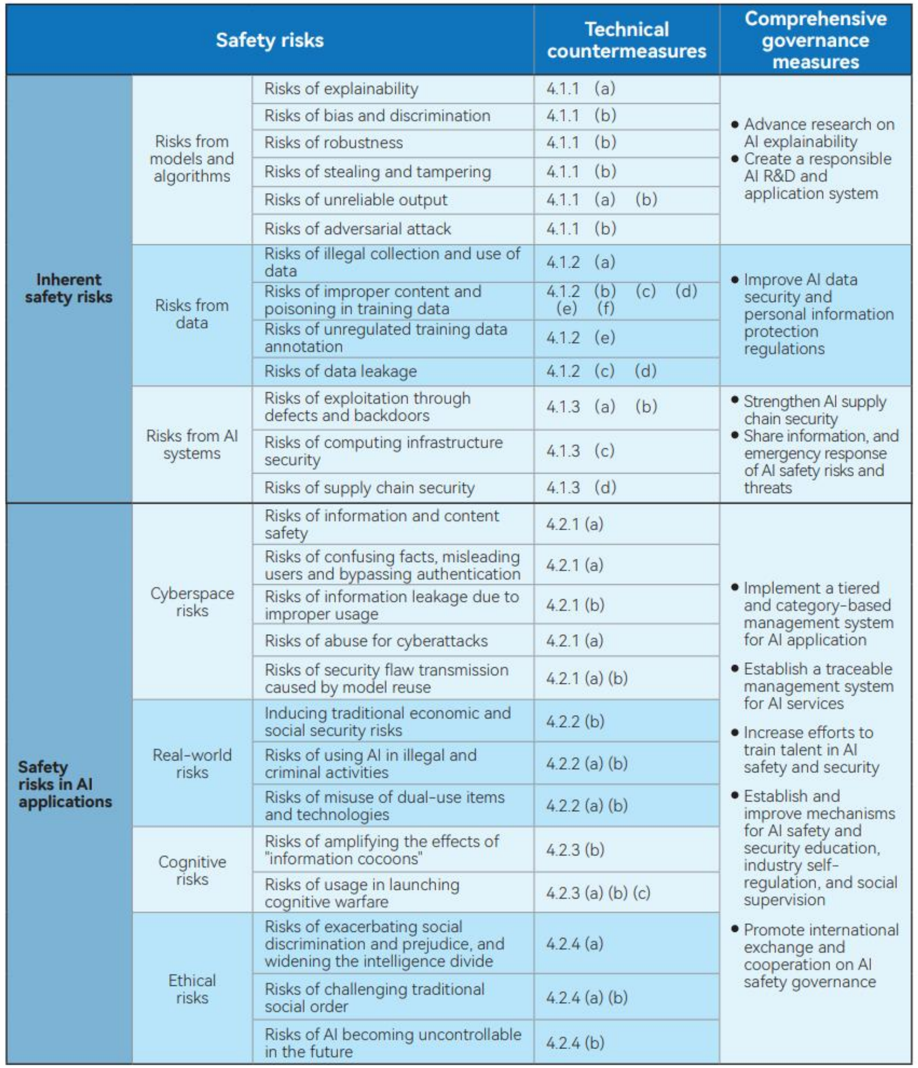
G. Security and Governance: GA Security; GB Governance

AI Governance/Safety & Security - TC260-Working Group of Emerging Technology Standardization (WG ETS)

Global Artificial Intelligence Governance Initiative by China issued in 2023

support

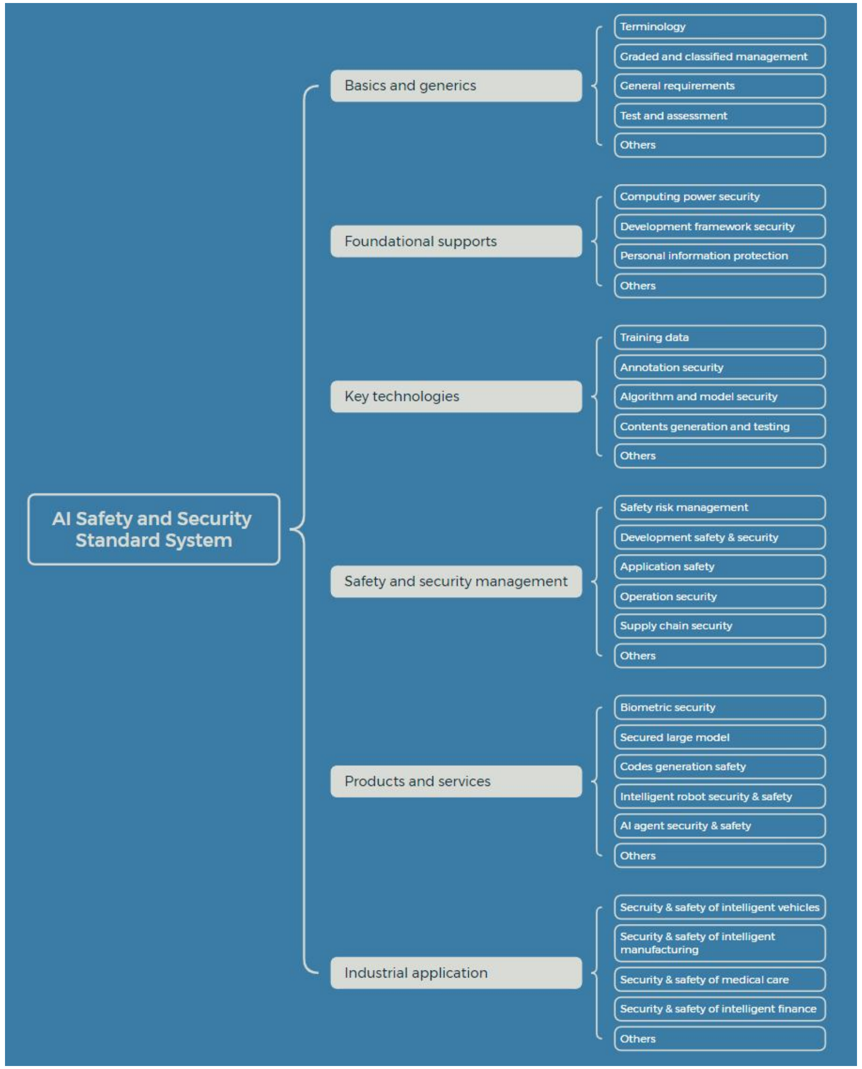
AI Governance Framework (released in 2024): Al Safety and Security Risks to Technical Countermeasures and Comprehensive Governance Measures



Safety risks			Technical countermeasures	Comprehensive governance measures
Inherent safety risks	Risks from models and algorithms	Risks of explainability	4.1.1 (a)	• Advance research on AI explainability • Create a responsible AI R&D and application system
		Risks of bias and discrimination	4.1.1 (b)	
		Risks of robustness	4.1.1 (b)	
		Risks of stealing and tampering	4.1.1 (b)	
		Risks of unreliable output	4.1.1 (a) (b)	
		Risks of adversarial attack	4.1.1 (b)	
	Risks from data	Risks of illegal collection and use of data	4.1.2 (a)	• Improve AI data security and personal information protection regulations
		Risks of improper content and poisoning in training data	4.1.2 (b) (c) (d) (e) (f)	
		Risks of unregulated training data annotation	4.1.2 (e)	
		Risks of data leakage	4.1.2 (c) (d)	
	Risks from AI systems	Risks of exploitation through defects and backdoors	4.1.3 (a) (b)	• Strengthen AI supply chain security • Share information, and emergency response of AI safety risks and threats
		Risks of computing infrastructure security	4.1.3 (c)	
		Risks of supply chain security	4.1.3 (d)	
Safety risks in AI applications	Cyberspace risks	Risks of information and content safety	4.2.1 (a)	• Implement a tiered and category-based management system for AI application • Establish a traceable management system for AI services • Increase efforts to train talent in AI safety and security • Establish and improve mechanisms for AI safety and security education, industry self-regulation, and social supervision • Promote international exchange and cooperation on AI safety governance
		Risks of confusing facts, misleading users and bypassing authentication	4.2.1 (a)	
		Risks of information leakage due to improper usage	4.2.1 (b)	
		Risks of abuse for cyberattacks	4.2.1 (a)	
		Risks of security flaw transmission caused by model reuse	4.2.1 (a) (b)	
	Real-world risks	Inducing traditional economic and social security risks	4.2.2 (b)	
		Risks of using AI in illegal and criminal activities	4.2.2 (a) (b)	
		Risks of misuse of dual-use items and technologies	4.2.2 (a) (b)	
	Cognitive risks	Risks of amplifying the effects of "information cocoons"	4.2.3 (b)	
		Risks of usage in launching cognitive warfare	4.2.3 (a) (b) (c)	
	Ethical risks	Risks of exacerbating social discrimination and prejudice, and widening the intelligence divide	4.2.4 (a)	
		Risks of challenging traditional social order	4.2.4 (a) (b)	
		Risks of AI becoming uncontrollable in the future	4.2.4 (b)	

support

AI Safety and Security Standard System (Draft in 2024)



AI Safety and Security Standard System

Basics and generics
- Terminology
- Graded and classified management
- General requirements
- Test and assessment
- Others

Foundational supports
- Computing power security
- Development framework security
- Personal information protection
- Others

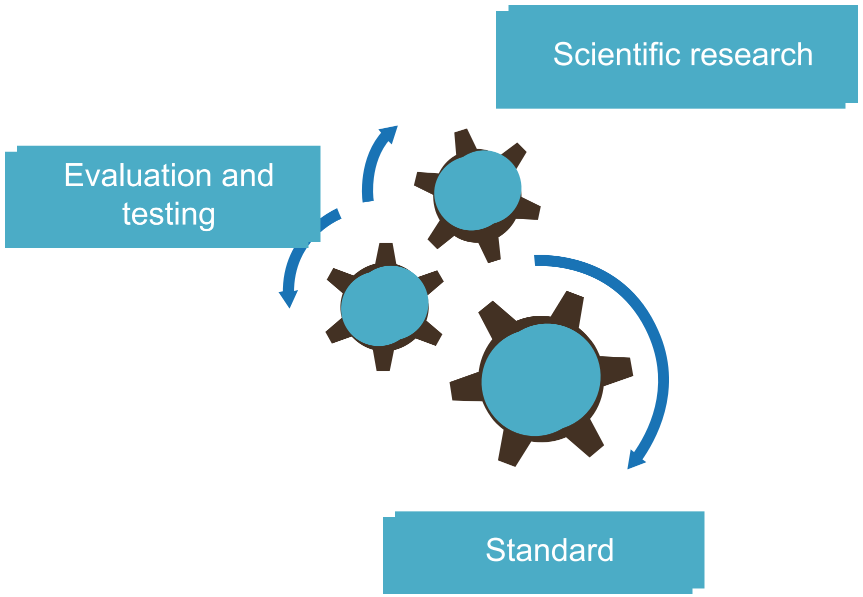
Key technologies
- Training data
- Annotation security
- Algorithm and model security
- Contents generation and testing
- Others

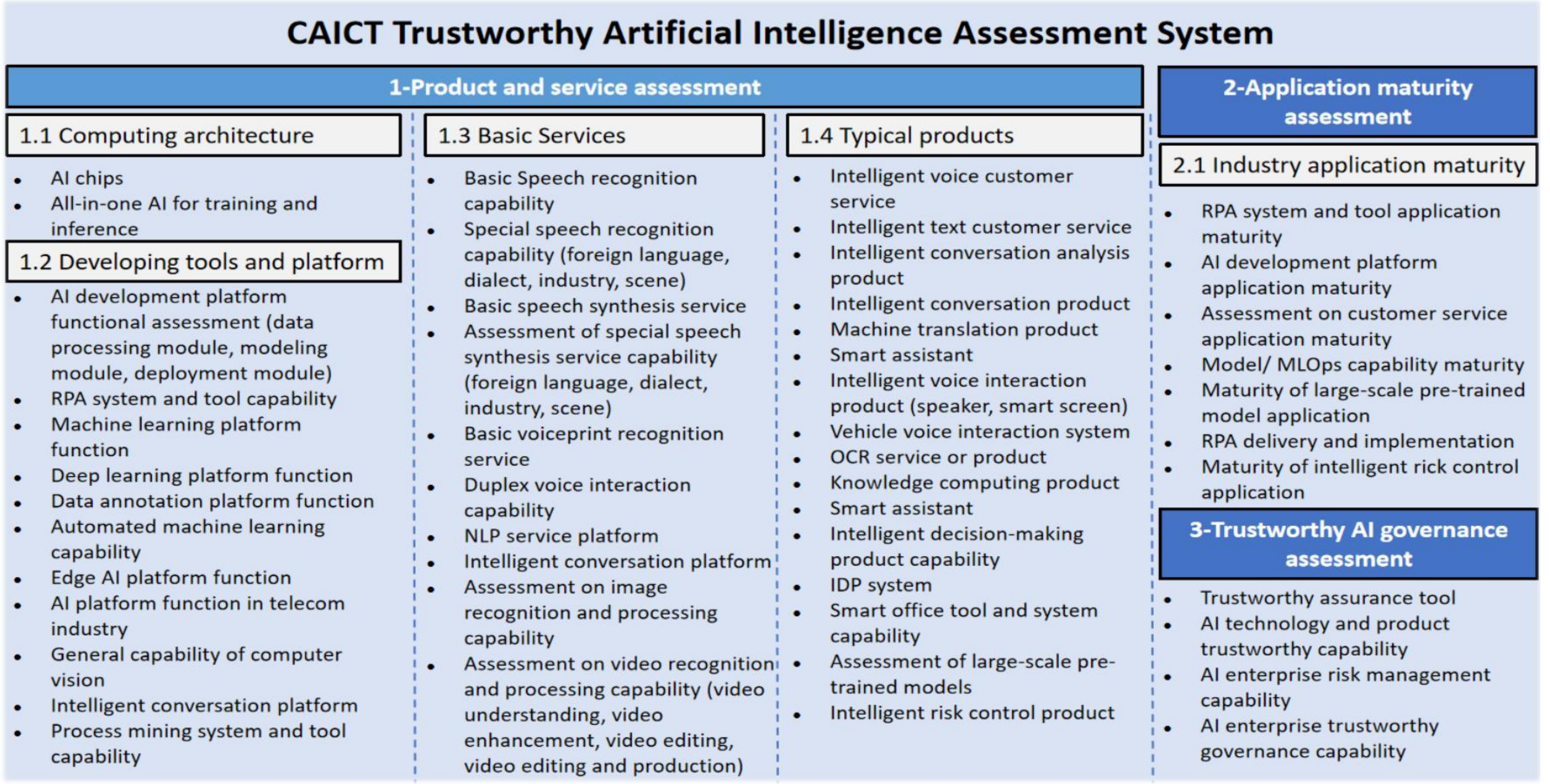
Safety and security management
- Safety risk management
- Development safety & security
- Application safety
- Operation security
- Supply chain security
- Others

Products and services
- Biometric security
- Secured large model
- Codes generation safety
- Intelligent robot security & safety
- AI agent security & safety
- Others

Industrial application
- Security & safety of intelligent vehicles
- Security & safety of intelligent manufacturing
- Security & safety of medical care
- Security & safety of intelligent finance
- Others

China AI Standardization - **AIIA** (Aritifical Intelligence Industry Alliance)





CAICT Trustworthy Artificial Intelligence Assessment System

1-Product and service assessment

1.1 Computing architecture

- AI chips
- All-in-one AI for training and inference

1.2 Developing tools and platform

- AI development platform functional assessment (data processing module, modeling module, deployment module)
- RPA system and tool capability
- Machine learning platform function
- Deep learning platform function
- Data annotation platform function
- Automated machine learning capability
- Edge AI platform function
- AI platform function in telecom industry
- General capability of computer vision
- Intelligent conversation platform
- Process mining system and tool capability

1.3 Basic Services

- Basic Speech recognition capability
- Special speech recognition capability (foreign language, dialect, industry, scene)
- Basic speech synthesis service
- Assessment of special speech synthesis service capability (foreign language, dialect, industry, scene)
- Basic voiceprint recognition service
- Duplex voice interaction capability
- NLP service platform
- Intelligent conversation platform
- Assessment on image recognition and processing capability
- Assessment on video recognition and processing capability (video understanding, video enhancement, video editing, video editing and production)

1.4 Typical products

- Intelligent voice customer service
- Intelligent text customer service
- Intelligent conversation analysis product
- Intelligent conversation product
- Machine translation product
- Smart assistant
- Intelligent voice interaction product (speaker, smart screen)
- Vehicle voice interaction system
- OCR service or product
- Knowledge computing product
- Smart assistant
- Intelligent decision-making product capability
- IDP system
- Smart office tool and system capability
- Assessment of large-scale pre-trained models
- Intelligent risk control product

2-Application maturity assessment

2.1 Industry application maturity

- RPA system and tool application maturity
- AI development platform application maturity
- Assessment on customer service application maturity
- Model/ MLOps capability maturity
- Maturity of large-scale pre-trained model application
- RPA delivery and implementation
- Maturity of intelligent rick control application

3-Trustworthy AI governance assessment

- Trustworthy assurance tool
- AI technology and product trustworthy capability
- AI enterprise risk management capability
- AI enterprise trustworthy governance capability

Major outcome:

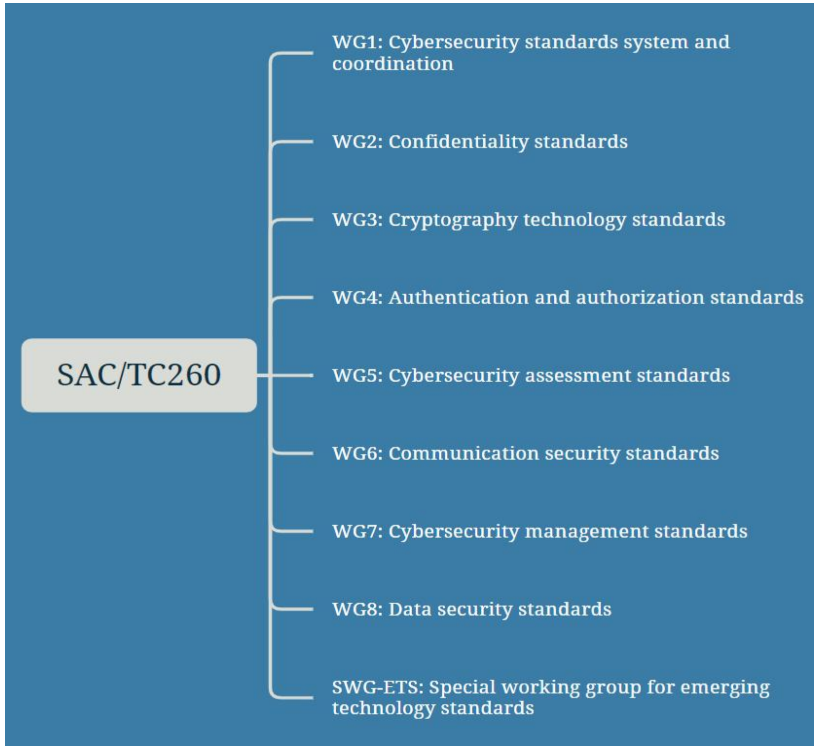
- Systematic comprehensive research on artificial intelligence has been carried out.
- A number of achievements such as the *White Paper on Artificial Intelligence* and the *White Paper on Trustworthy Artificial Intelligence* issued by CAICT (that runs the AIIA) have been translated and reproduced by internationally renowned think tanks.
- Establishing AI test technology platform and evaluation service system via three dimensions of cutting-edge technology, technology applications and trustworthy governance.
- Establishing "Trusted AI" standard system, actively promoting the conversion of relevant AI standards to ITU-T and IEEE standards and promoting international exchanges and cooperation.

03

Cybersecurity in General – TC260

Statistics:

- **400+** national security standards have been issued, covering CIIO protection, cybersecurity products, data security.
- **60+** Chine-led international standards accounting for 18% of the total work of ISO/IEC JTC 1/SC27
- **2** newly established working groups: WG8 (Data Security), and the Special Working Group for Emerging Technology Standardization.



SAC/TC260

WG1: Cybersecurity standards system and coordination

WG2: Confidentiality standards

WG3: Cryptography technology standards

WG4: Authentication and authorization standards

WG5: Cybersecurity assessment standards

WG6: Communication security standards

WG7: Cybersecurity management standards

WG8: Data security standards

SWG-ETS: Special working group for emerging technology standards

Priorities for the future:

1. **Alignment and coordination**: standards support legislation, coordination between standards, and standard optimization
2. Support to the construction of **cybersecurity defense system**: responsibility focus adjustment (pure enterprise responsibility to shared responsibility between enterprise and government authorities) + cybersecurity product interconnection
3. Provide guidelines to the development of **new technologies** and applications via standards: artificial intelligence, big data, Internet of Things, blockchain and quantum communication.

	Number of Chinese Company	Number of Foreign Company	In total
WG3 Cryptology	109	3	112
WG4 Authentication and authorization	135	10	145
WG5 Cybersecurity and assessment	371	38	409
WG6 Communication Security	107	14	121
WG7 Cybersecurity Management	308	27	335
WG8 Data Security	400	29	429
SWG-ETS Special Working Group of Emerging Technology Standardization	135	10	145

03

Cybersecurity: - Data Security and Personal Information Protection

National Standards for Data Security

Security requirements

- GB/T 43697-2024 Rules for data classification and grading
- GB/T 41479-2022 Network data processing security requirements
- GB/T 42012-2022 Data security requirements for instant messaging services
- GB/T 42013-2022 Data security requirements for express logistics services
- GB/T 42014-2022 Data security requirements for online shopping services
- GB/T 39477-2020 Government information sharing—Data security technology requirements
- GB/T 41871-2022 Security requirements for processing of motor vehicle data
- GB/T 42015-2022 Data security requirements for internet payment services
- GB/T 42016-2022 Data security requirements for online audio and video services
- GB/T 42017-2022 Data security requirements for online ride-hailing services
- GB/T 35274-2023 Security capability requirements for big data services
- GB/T 37932 Security requirements for data transaction service (under revision)
- Requirements for data security protection (under development)
- Public data opening security requirements (under development)
- Security requirements for government data processing (under development)
- Technical requirements of second-hand electronic product information erasure (under development)

Framework and guidelines

- 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
- General framework for the confidential computing (under development)
- Technical method for risk monitoring of data Application Programming Interface (under development)
- Technical implementation guideline of digital watermarking (under development)

Testing and assessment

- GB/T 37988-2019 Data security capability maturity model
- Risk assessment approaches for data security (under development)
- Capacity requirements for assessment organization of data security (under development)

Cybersecurity: - Data Security and Personal Information Protection

National Standards Personal Information Protection

Security requirements

- GB/T 35273-2020 Personal information security specification
- GB/T 41391-2022 Basic requirements for collecting personal information in mobile internet applications
- GB/T 41819-2022 Security requirements of face recognition data
- GB/T 41807-2022 Security requirements of voiceprint recognition data
- GB/T 43445-2023 Basic security requirements for pre-installed applications on smart mobile terminals
- GB/T 40660-2021 General requirements for biometric information protection
- GB/T 41806-2022 Security requirements of genetic recognition data
- GB/T 43435-2023 Security requirements for software development kit (SDK) in mobile internet applications (App)
- GB/T 44588-2024 Personal information processing rules of internet platforms, products and services
- Personal Information Protection Compliance Audit Requirements (under development)
- Security requirements for Automated decision making based on personal information (under development)
- Security requirements for processing of sensitive personal information (under development)
- Requirements for large Internet companies' internal personal information protection supervision agency (under development)
- Requirements for personal information transfer based on request of personal information subjects (under development)

Framework and guidelines

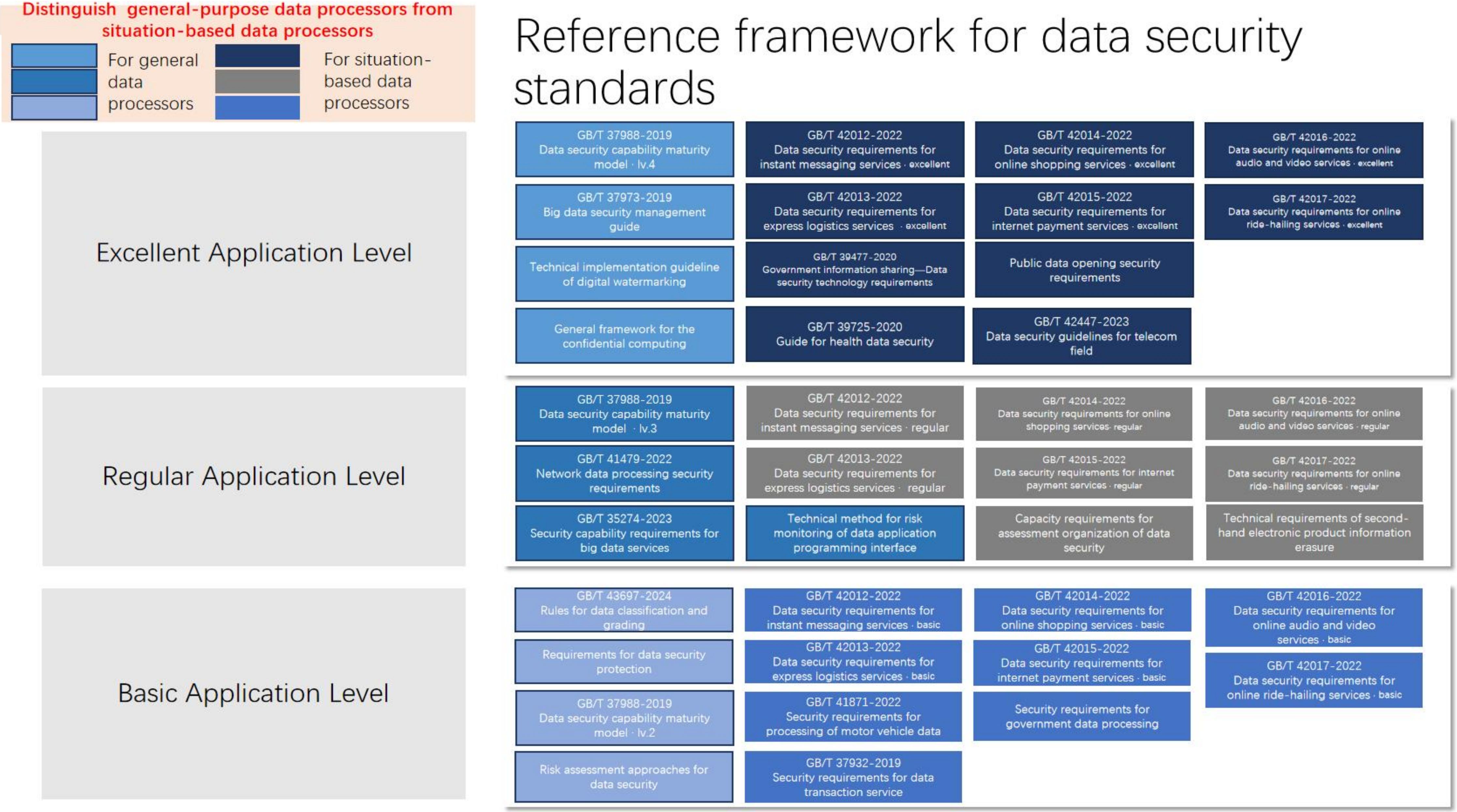
- GB/T 37964-2019 Guide for de-identifying personal information
- GB/T 41817-2022 Guidelines for personal information security engineering
- GB/T 41574-2022 Code of practice for protection of personal information in public clouds
- GB/T 42574-2023 Implementation guidelines for notices and consent in personal information processing
- GB/T 43739-2024 Audit and management guide for personal information processing normativeness of mobile internet applications in App stores
- Personal information processing management guide for mobile internet applications of smart mobile devices (under development)
- Guidance on social responsibility of data security and personal information protection (under development)

Testing and assessment

- GB/T 39335-2020 Guidance for personal information security impact assessment
- GB/T 42460-2023 Guide for evaluating the effectiveness of personal information de-identification
- GB/T 42582-2023 Personal information security testing and evaluation specification in mobile internet applications（App）
- Security certification requirements for cross-border processing activity of personal information (under development)

Cybersecurity: Data Security and Personal Information Protection

- TC260 Data Security Standards Enhancement Program (DSEP): Data Security



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

- 🟦🟦🟦 For general data processors
- ⬛⬛🟦 For situation-based data processors

Reference framework for data security standards

Excellent Application Level

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

Regular Application Level

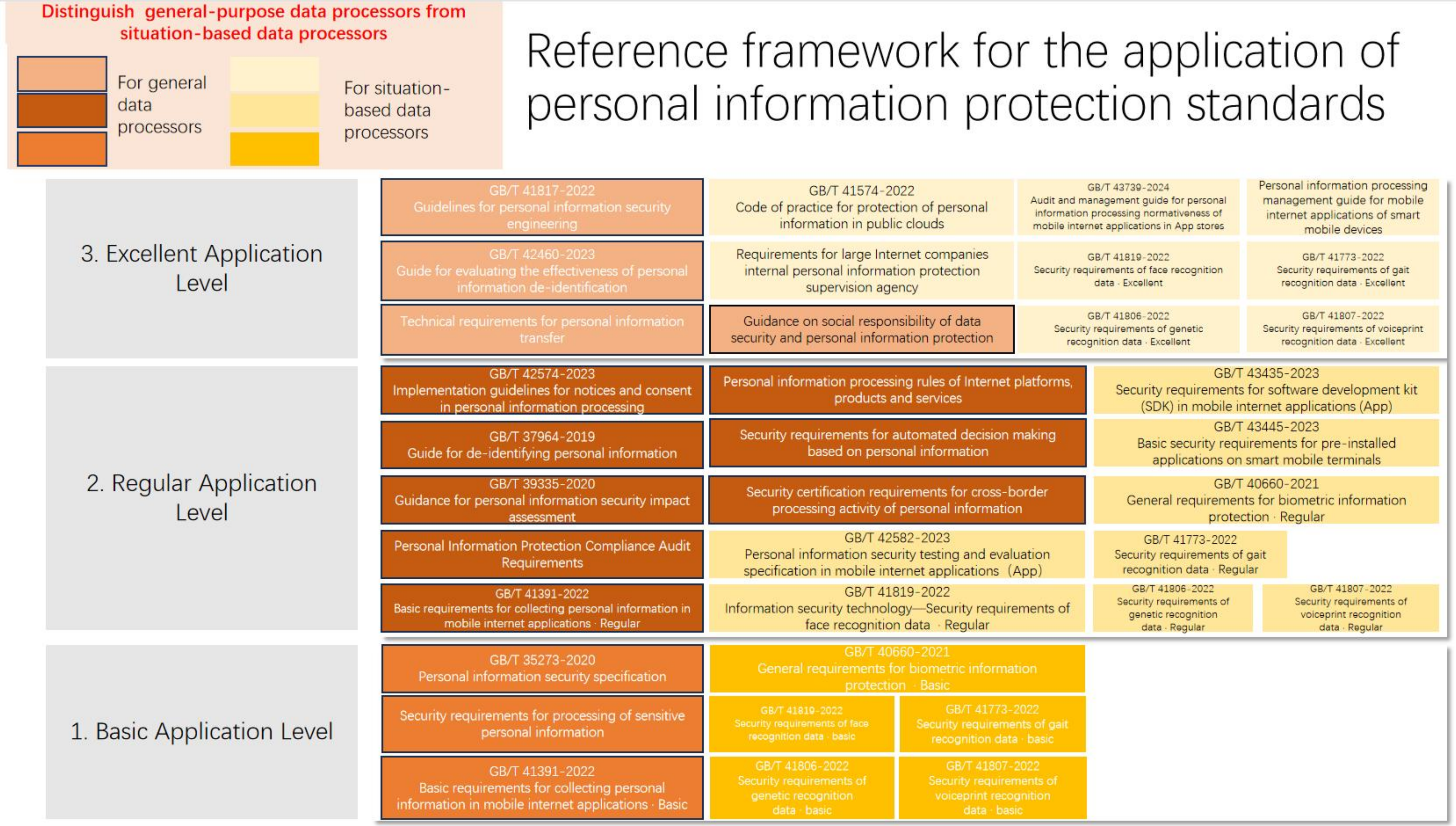
- GB/T 37988-2019 Data security capability maturity model · lv.3
- GB/T 41479-2022 Network data processing security requirements
- GB/T 35274-2023 Security capability requirements for big data services
- GB/T 42012-2022 Data security requirements for instant messaging services · regular
- GB/T 42013-2022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

Basic Application Level

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

Cybersecurity: Data Security and Personal Inforamtion Protection

- TC260 Data Security Standards Enhancement Program (DSEP): Personal Information Protection



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

For general data processors

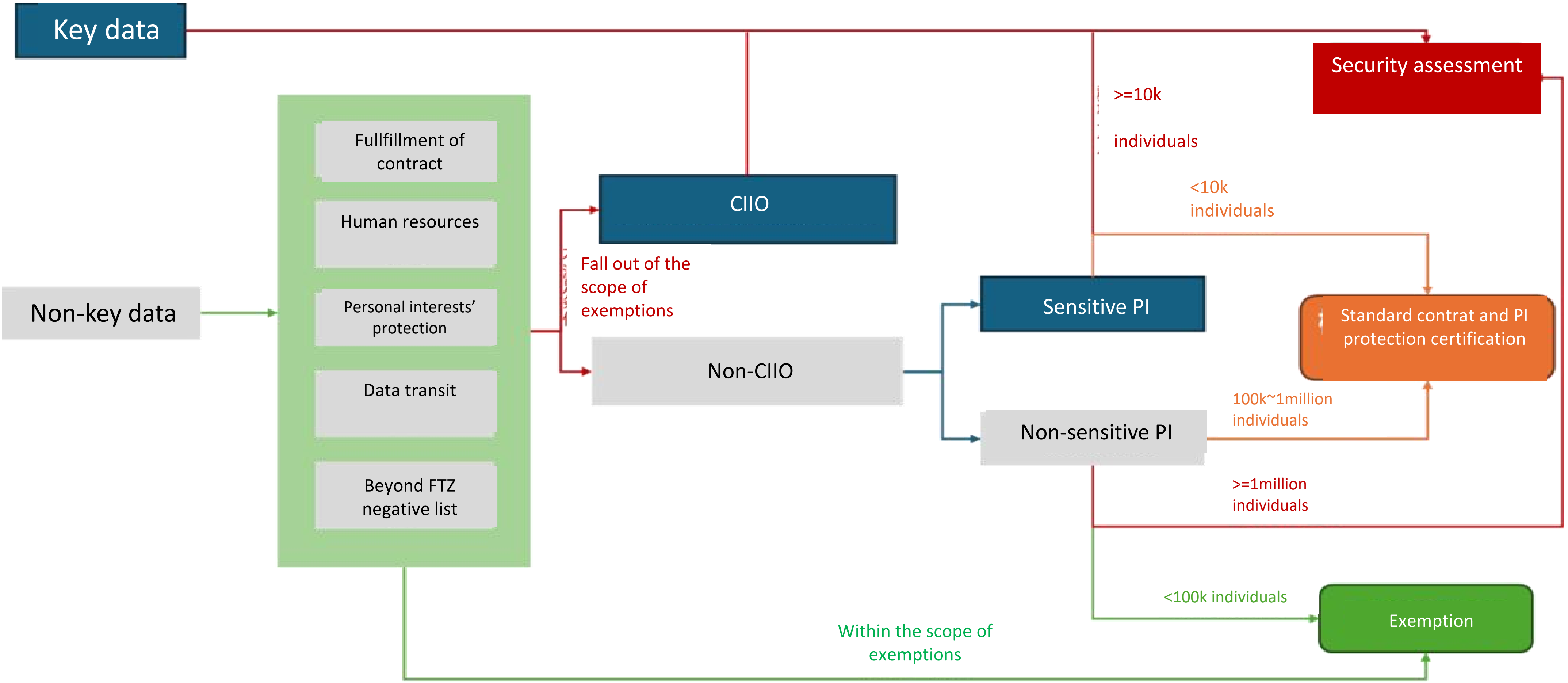
For situation-based data processors

Reference framework for the application of personal information protection standards

3. Excellent Application Level	GB/T 41817-2022 Guidelines for personal information security engineering	GB/T 41574-2022 Code of practice for protection of personal information in public clouds	GB/T 43739-2024 Audit and management guide for personal information processing normativeness of mobile internet applications in App stores	Personal information processing management guide for mobile internet applications of smart mobile devices
	GB/T 42460-2023 Guide for evaluating the effectiveness of personal information de-identification	Requirements for large Internet companies internal personal information protection supervision agency	GB/T 41819-2022 Security requirements of face recognition data · Excellent	GB/T 41773-2022 Security requirements of gait recognition data · Excellent
	Technical requirements for personal information transfer	Guidance on social responsibility of data security and personal information protection	GB/T 41806-2022 Security requirements of genetic recognition data · Excellent	GB/T 41807-2022 Security requirements of voiceprint recognition data · Excellent
2. Regular Application Level	GB/T 42574-2023 Implementation guidelines for notices and consent in personal information processing	Personal information processing rules of Internet platforms, products and services	GB/T 43435-2023 Security requirements for software development kit (SDK) in mobile internet applications (App)	
	GB/T 37964-2019 Guide for de-identifying personal information	Security requirements for automated decision making based on personal information	GB/T 43445-2023 Basic security requirements for pre-installed applications on smart mobile terminals	
	GB/T 39335-2020 Guidance for personal information security impact assessment	Security certification requirements for cross-border processing activity of personal information	GB/T 40660-2021 General requirements for biometric information protection · Regular	
	Personal Information Protection Compliance Audit Requirements	GB/T 42582-2023 Personal information security testing and evaluation specification in mobile internet applications （App）	GB/T 41773-2022 Security requirements of gait recognition data · Regular	
	GB/T 41391-2022 Basic requirements for collecting personal information in mobile internet applications · Regular	GB/T 41819-2022 Information security technology—Security requirements of face recognition data · Regular	GB/T 41806-2022 Security requirements of genetic recognition data · Regular	GB/T 41807-2022 Security requirements of voiceprint recognition data · Regular
1. Basic Application Level	GB/T 35273-2020 Personal information security specification	GB/T 40660-2021 General requirements for biometric information protection · Basic		
	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	

Cross-border Data Transfer:

- Flow chart of Data Cross-border Transfer Mechanisms and Exemption

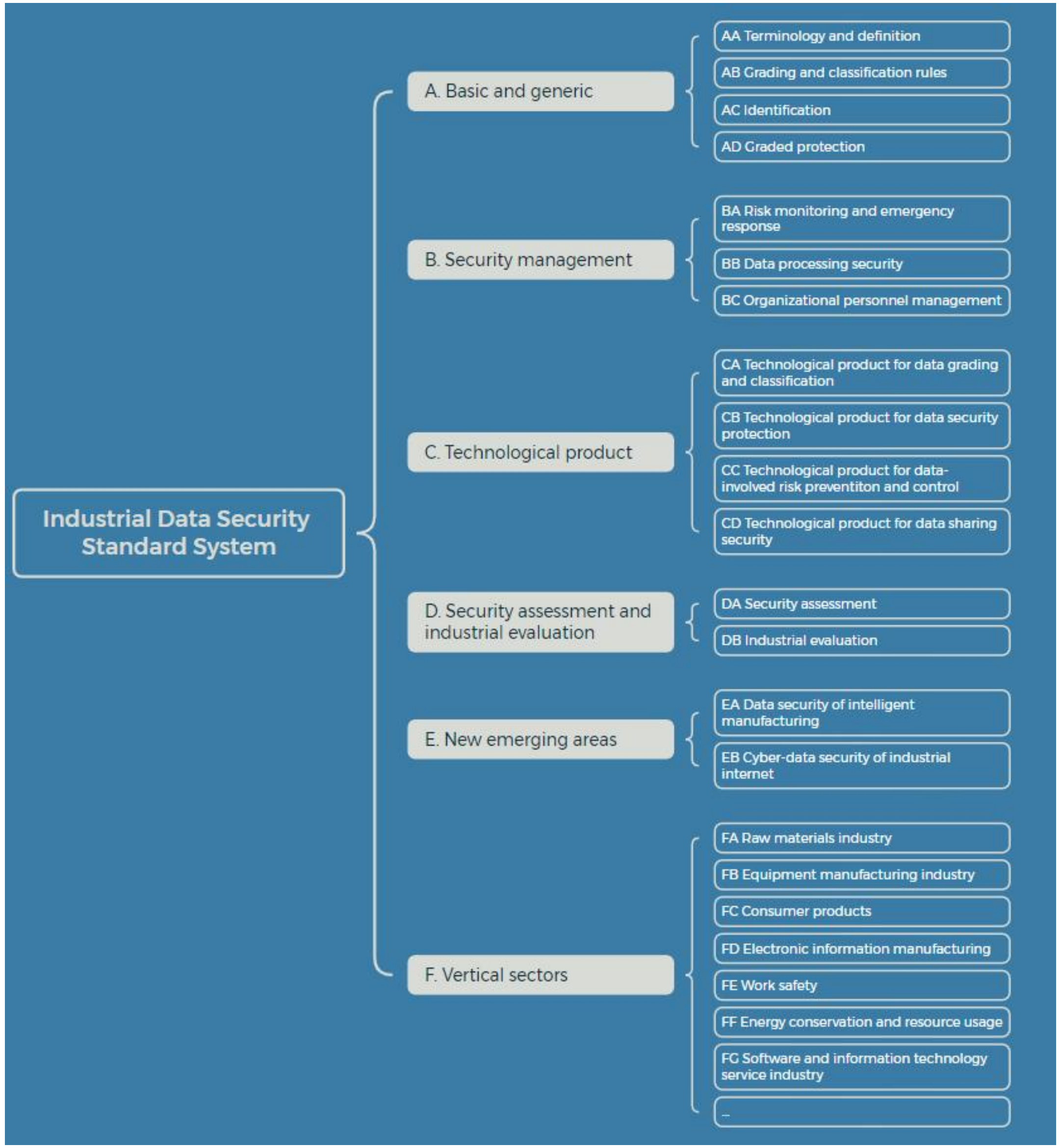


Cross-border Data Transfer:

- Major Standards for Cross-border Data Transfer

• 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
• How to conduct personal information protection assessment?	• GB/T 39335-2020 Guidance for personal information security impact assessment
• Certification basis and correspondent standards	• GB/T 35273 Personal information security specification • TC260-PG-20222A Security certification specification for cross-border processing of personal informatio • 20230255-T-469 Security certification requirements for cross-border processing activity of personal information (draft for approval)
• How to inform and obtain the individual’s separate consent?	• GB/T 42574-2023 Implementation guidelines for notices and consent in personal information processing
• 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

Cybersecurity Industrial Data



Industrial Data Security Standard System

A. Basic and generic
- AA Terminology and definition
- AB Grading and classification rules
- AC Identification
- AD Graded protection

B. Security management
- BA Risk monitoring and emergency response
- BB Data processing security
- BC Organizational personnel management

C. Technological product
- CA Technological product for data grading and classification
- CB Technological product for data security protection
- CC Technological product for data-involved risk preventiton and control
- CD Technological product for data sharing security

D. Security assessment and industrial evaluation
- DA Security assessment
- DB Industrial evaluation

E. New emerging areas
- EA Data security of intelligent manufacturing
- EB Cyber-data security of industrial internet

F. Vertical sectors
- FA Raw materials industry
- FB Equipment manufacturing industry
- FC Consumer products
- FD Electronic information manufacturing
- FE Work safety
- FF Energy conservation and resource usage
- FG Software and information technology service industry
- ...

Figure: Table of Industrial Data Security Standard System (2023 Version)

By 2024:

- Initially establish a data security standard system for the industrial sector;
- Promote the application of standards in key industries and major enterprises;
- Develop more than 30 national, industry, or association standards related to data security.

By 2026:

- Form a relatively complete data security standard system for the industrial sector;
- Fully implement the requirements of relevant laws, regulations, and policy systems on data security, providing strong support for key tasks in industrial data security;
- Develop more than 100 national, industry, or association standards related to data security.

Cybersecurity Industrial Data

A. Basic and Generic

- GB/T 43697-2024 Data security technology — Rules for data classification and grading

C. Technology Product

- GB/T 39400-2020 Industrial data quality—General technical specification

D. Security assessment and industrial evaluation

- Risk assessment approaches for data security (under development)
- GB/T 37988-2019 Information security technology—Data security capability maturity model

F. Vertical Sectors

- GB 44495-2024 Technical requirements for vehicle cybersecurity
- GB/T 44464-2024 General requirements of vehicle data
- MH/T 2011—2019 Data specifications of unmanned aircraft cloud system
- GB/T 37037-2018 Data specification for wearable product
- GB/T 40685-2021 Information technology service—Data asset—Management requirements
- YD/T 3470-2019 File data security label specification for public cloud services
- YD/T 3797.1-2021 Cloud user data protection capability assessment method part 1: public clouds
- YD/T 3797.2-2020 Cloud user data protection capability assessment method Part 2:Private clouds

Standards List in 2024 (Status Updated): Published and Under Development

Industrial Field

- YDT 4981-2024 Guidelines for identification of key data in industrial field
- Data security protection requirements (under development)
- Specification for industrial field data security risk assessment (under development)

Telecom Field

- YD/T 3867-2024 Guidelines for identification of key data in telecommunication field
- Data security protection requirements (under development)
- YD/T 3956-2024 Specification for telecommunication field data security risk assessment

04

Overview of Data Regime in China

Trend of Development

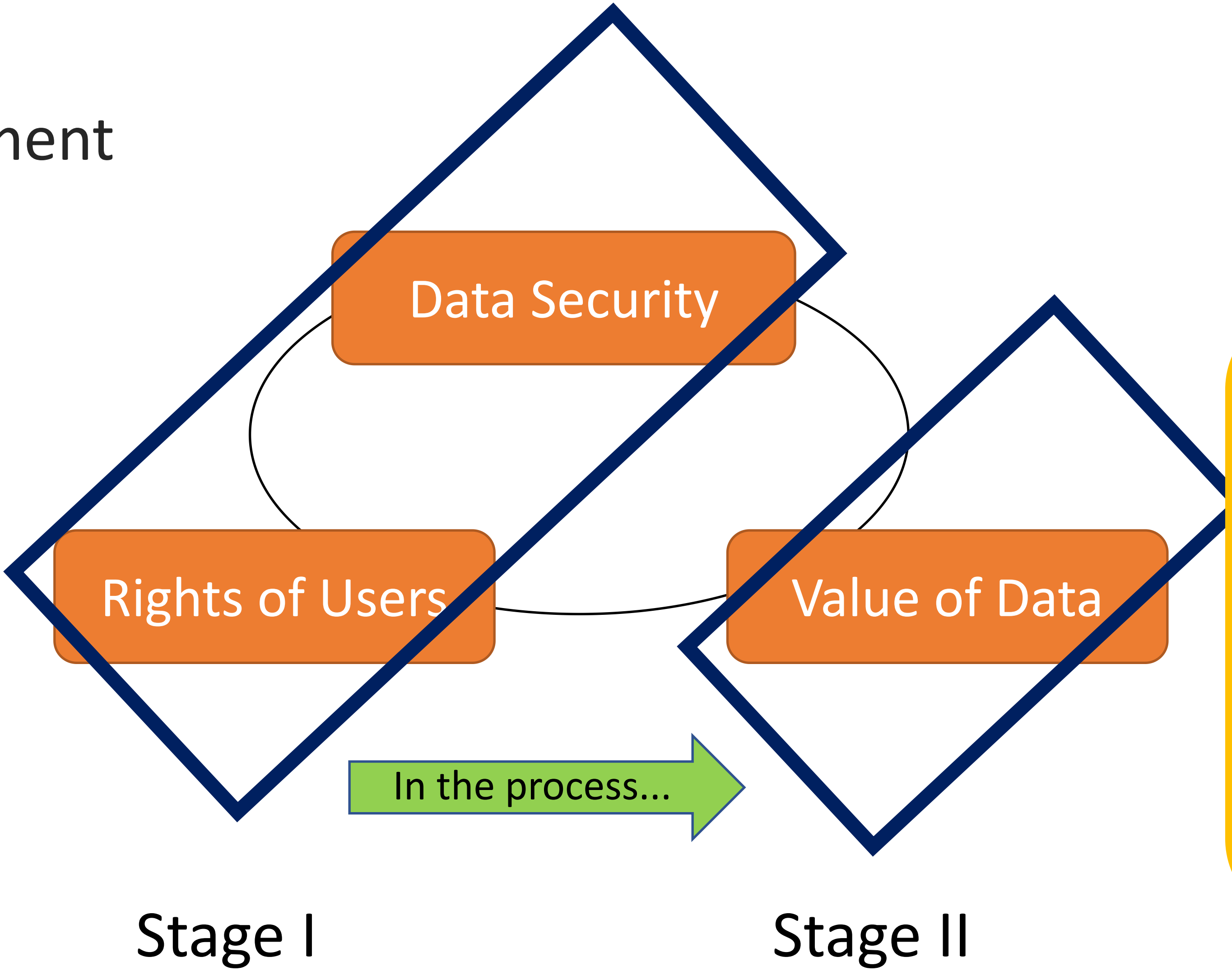
Major Regulations, Laws and Policies

Data Security:

- *National Security Law*
- *Cybersecurity Law*
- *Data Security Law*

Rights of Users:

- China's *Civil Code*
- *Personal Information Protection Law*



Major Regulations, Laws and Policies

Value of Data:

- *Guidelines on Building Basic Data Systems to Better Leverage the Role of Data as a Production Factor*
- Legislation at local level

04

Overview of Data Regime in China

Major moves:

a. Newly-established Governmental Agency:
National Data Administration
Established in **Oct 2023**

b. Nation-wise, the release of a new policy: ***Guidelines on Building Basic Data Systems to Better Leverage the Role of Data as a Production Factor* (Known as the 20 Data Measures)**

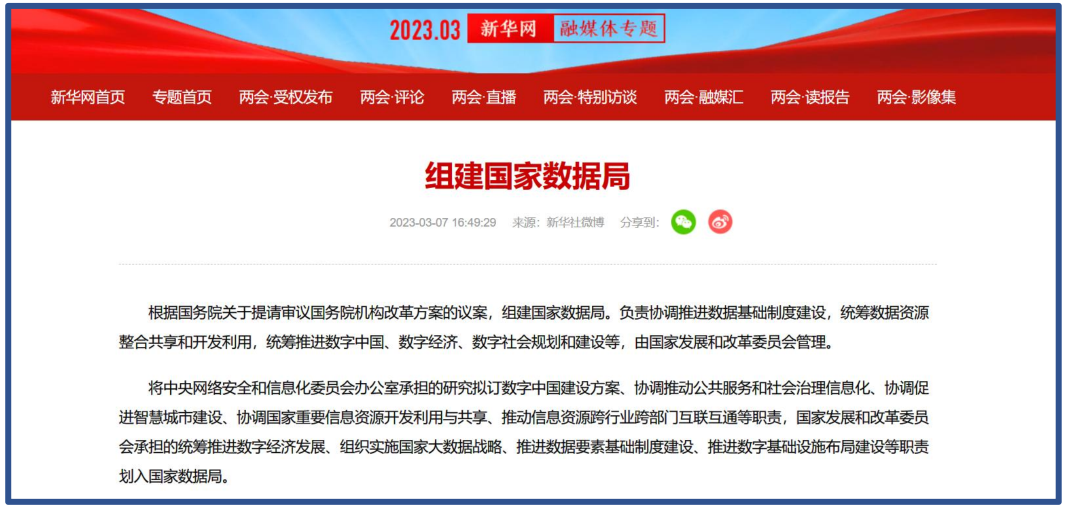
c. **Industry-specific administrative measures**

Background: Plan for Institutional Reform of the Party and State Released in **March 2023**

Responsibilities:

- coordinating and advancing the construction of basic data system
- coordinating the integration, sharing, development and utilization of data resources
- coordinating the planning and construction of digital China, digital economy and digital society.

Superior body: National Development and Reform Commission



组建国家数据局

2023-03-07 16:49:29　来源：新华社微博　分享到：

根据国务院关于提请审议国务院机构改革方案的议案，组建国家数据局。负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，由国家发展和改革委员会管理。

将中央网络安全和信息化委员会办公室承担的研究拟订数字中国建设方案、协调推动公共服务和社会治理信息化、协调促进智慧城市建设、协调国家重要信息资源开发利用与共享、推动信息资源跨行业跨部门互联互通等职责，国家发展和改革委员会承担的统筹推进数字经济发展、组织实施国家大数据战略、推进数据要素基础制度建设、推进数字基础设施布局建设等职责划入国家数据局。

04

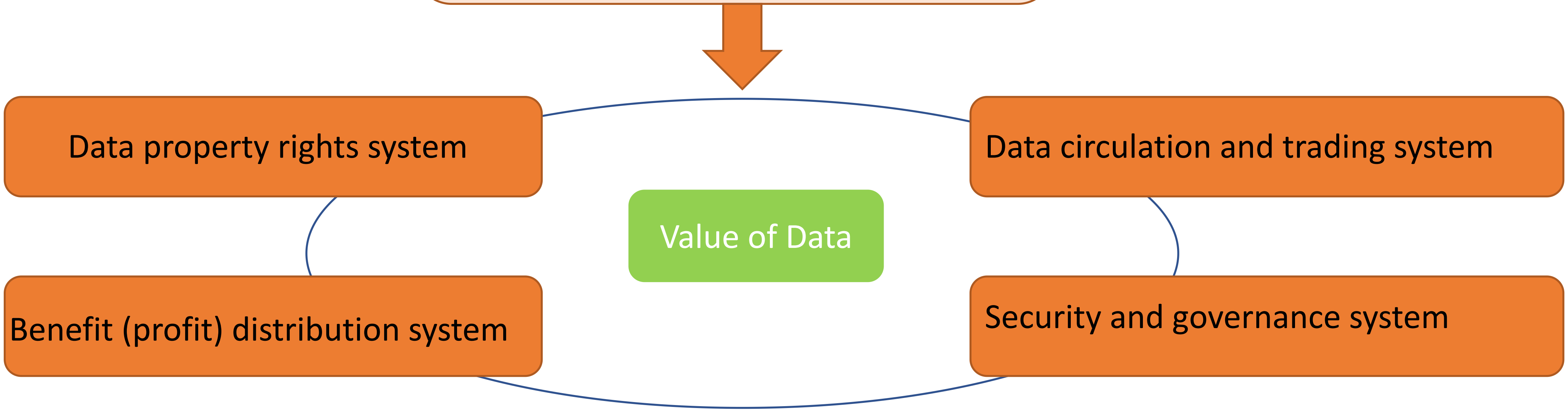
Overview of Data Regime in China

Major moves:

a. Newly-established Governmental Agency:
National Data Administration
Established in **Oct 2023**

b. Nation-wise, the release of the policy: ***Guidelines on Building Basic Data Systems to Better Leverage the Role of Data as a Production Factor*** **(Known as the 20 Data Measures) Dec 2022**

c. Industry-specific administrative measures



Data property rights system

Data circulation and trading system

Value of Data

Benefit (profit) distribution system

Security and governance system

04

Overview of Data Regime in China

Major moves:

a. Newly-established Governmental Agency:
National Data Administration

b. Nation-wise, the release of a new policy: *Guidelines on Building Basic Data Systems to Better Leverage the Role of Data as a Production Factor* **(Known as the 20 Data Measures)**

c. Industry-specific administrative measures

MIIT: Data Security Governance Framework in Industry and Information Sector

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

Data security

- key data identification
- core data identification
- Submission and Sharing of Data Security Risk Information
- Emergency Plan for Data Security Incidents
- Administrative Penalty Discretion
- Data Security Risk Assessments

04

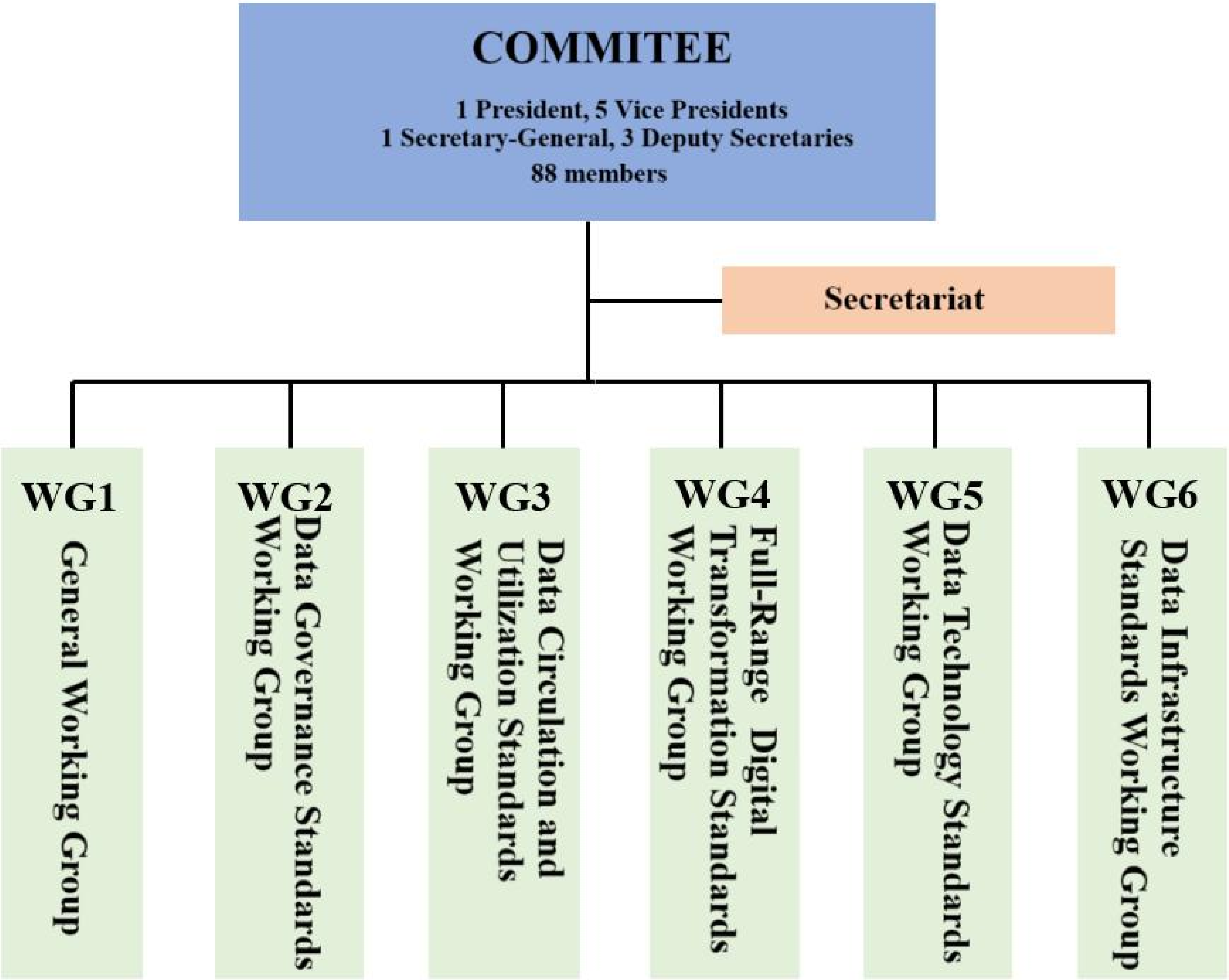
China Data Standardization

Newly Established in Oct 2024!

National Technical Committee on Data (SAC/TC609)

- Working scope: foundational standards for data resources, technology, circulation, smart cities, data infrastructure, and security in data utilization.
- Number of members: 98 members
- Mirroring ISO/IEC JTC1/SC32 (Data management and interchange), ISO/IEC JTC1/SC42/WG2 (Data), ISO/IEC JTC1/WG11 (Smart Cities), and IEC/SyC Smart Cities (Electrotechnical aspects of Smart Cities)

- *Appraoching Cooperation with CENCENELEC JTC 25 'Data management, Dataspaces, Cloud and Edge'.*



COMMITEE

1 President, 5 Vice Presidents
1 Secretary-General, 3 Deputy Secretaries
88 members

Secretariat

WG1 General Working Group

WG2 Data Governance Standards Working Group

WG3 Data Circulation and Utilization Standards Working Group

WG4 Full-Range Digital Transformation Standards Working Group

WG5 Data Technology Standards Working Group

WG6 Data Infrastructure Standards Working Group

04

Data standardization organization

A list of
prepare
Totall

#	Standard /plan no.	Standard name/project name
	GB/T 35295-2017	Information technology—Bigdata—Terminology
	GB/T 35589-2017	Information technology-Big data-Technical reference model
	GB/T 36343-2018	Information technology-Data transaction service platform Transaction data description
	GB/T 37728-2019	Information technology-Data transaction service platform General functional requirements
	…	……
1	GB/T 42450-2023	Information technology-Big data-Planning of data resource
2	GB/T 44109-2024	Information technology-Big data-Guidelines of data governance implementation
3	GB/T 44216-2024	Information technology-Technical requirements for batch fusion computing of big data
	…	……
31	20214285-T-469	Information technology-big data-data assets value evaluation
32	20220415-T-469	Information technology-big data-Evaluation of data service capability-Part 1: Evaluation model
33	20241469-T-469	Information technology-big data-Core metadata of data assets
	…	……

,
k,

t

a

ıl

t
n

05

Industry IOT – Intelligent Manufacturing

Latest Standardization-related Policies

***The 14th Five-Year Plan for the Development of Intelligent Manufacturing*,** issued in Dec 2021 by MIIT, SAMR, and 6 other ministries, providing a guidance for the development of intelligent manufacturing (IM) through the next five years (2021-2025)

- establish IM **application standards systems for the sectors** of textile, petrochemicals, building materials, automobile, aerospace, shipbuilding, power equipment, urban rail transport, household appliance, food, steel, nonferrous metals, and new energy. Accelerate the development of industry application standards,
- Promote the development **of fundamental and key technical standards** for digital twins, data dictionaries, human-machine collaboration, intelligent supply chains, system reliability, and the integration of information security and functional safety;
- Conduct **pilot projects on the application** of IM standards, focusing on areas such as intelligent workshop/factory construction, new model applications, supply chain collaboration, and new technology applications.
- Continue to **strengthen Sino-German cooperation**, expand cooperation with Japan, the UK, and others, actively participate in international standardization activities.

The Guidelines for the Construction of the National Intelligent Manufacturing Standard System (2021) issued by MIIT and SAC in Nov 2021, providing direction and framework for the development of IM standards in China

National IM Coordination & Promotion WG,
MIIT,
SAC,
etc.

Implementation

National IM Standardization General Group,
CESI,
ITEI,
CAICT,
CNIS, and other SDOs

Latest Progress

MIIT has released the 'IM standard system construction guidelines' for petrochemicals, iron and steel, non-ferrous metal, building materials, and chemical industry as of **September 2024.**

China has developed 369 national standards and 38 international standards *. In its *China Intelligent Manufacturing (IM) Development Report: Standardization*, released in **November 2022,** CESI identified 263 key IM national and sector standards. Of these, 212 have been finalized, while 35 are currently at various stages of development.

MIIT and SAC carried out IM standards application pilot projects every year. **In 2023,** 78 pilot projects application were submitted to MIIT and SAC for approval.

Sino-Germany Industrie 4.0/Intelligent Manufacturing SWG, Sino-Japan IM industry cooperation demonstration zone. China-led international IM standards has reached 48 by April, 2023. *

* Source: 2023 Plenary Meeting of National IM Standardization General Group and Expert Advisory Group

05

Industry IOT – Industrial Internet

Latest Standardization-related Policies

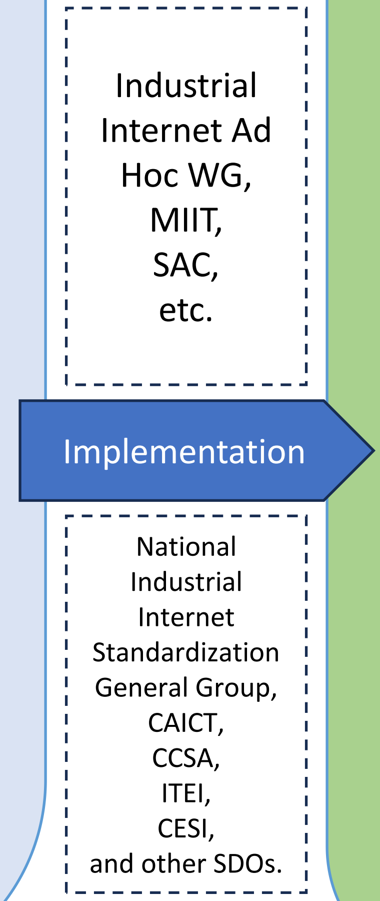
The Industrial Internet Innovative Development Action Plan (2021-2023), issued by MIIT in Jan 2021

- In line with new technology applications such as 5G, edge computing, and artificial intelligence, and the trends in industrial development, **improve the industrial internet standards system by defining key areas and directions for standardization**.
- Accelerate the development of fundamental, common standards such as network, platform, and security system architectures, general requirements, and terminology definitions. Expedite the formulation of key technical standards for '5G + Industrial Internet,' network information models, industrial big data, and security protection. Speed up the creation of application standards for key industries, including raw materials, equipment, and electronic information.

The Guidelines for Constructing a Comprehensive Industrial Internet Standards System (2021) issued by MIIT in Dec 2021, laying down direction and framework for the development of industrial internet standards in China

Annual *Work Plan of Industrial Internet Ad Hoc WG*. In its 2024 edition, the WG proposes to

- Revise the *Guidelines for Constructing Comprehensive Industrial Internet Standards System*.
- In terms of technology, promote the development of >3 national standards in areas of new industrial networks, identification and resolution, and blockchain. Additionally, advance the formulation and release of >10 key standards for active identification carriers, industrial equipment data dictionaries, industry metadata, and green low-carbon identification
- In terms of application, promote the initiation of >2 sector standards for 5G industrial integration terminals.
- In term of industrial chains, promote the development of standards for digital transformation of industrial parks, collaboration within industrial clusters, and chain-based empowerment
- In terms of platform and data, advance the initiation of standards of *'Industrial Internet Platform Park Application Level Evaluation'* and the development of related standards, including industrial internet platform reference architecture, digital management of safety production, industrial equipment data dictionaries, industrial equipment cloud integration, data sharing and exchange, and data governance.



Industrial Internet Ad Hoc WG, MIIT, SAC, etc.

Implementation

National Industrial Internet Standardization General Group, CAICT, CCSA, ITEI, CESI, and other SDOs.

Latest Progress *

In 2023/2024, China initiated 25+ national standard projects and 64 sector standard projects, advancing the development of sub-standard systems for industrial internet applications across various industries. To promote the implementation of industrial internet standards, China selected 40 demonstration cases from 170 applications.

Intention- to have ***The Guidelines for Constructing a Comprehensive Industrial Internet Standards System (2024)***

To date, China has published 10+ national standards for the industrial internet, including GB/T 42021 for general network architecture. Additionally, more than 40 national standards projects are currently in progress. SAC will focus on setting standards for the deep integration of the industrial internet in various industries and will work to promote the adoption and application of the developed standards.

* Source: 2023 Summary Meeting and 2024 First Work Meeting of the National Industrial Internet Standards General Group

05

Smart Standards

China stressed the development of smart standards in multiple policies. The recent one is the *Action plan for developing informatization standards (2024-2027)* released by MIIT in June 2024. It requires making breakthrough on key technologies such as machine-readable standards, open-source standards, and the digital validation of standards.

Currently, the following two organizations play a leading role in the research of smart standards.

National Working Group for the digitalization of Standards (SAC/SWG 29)

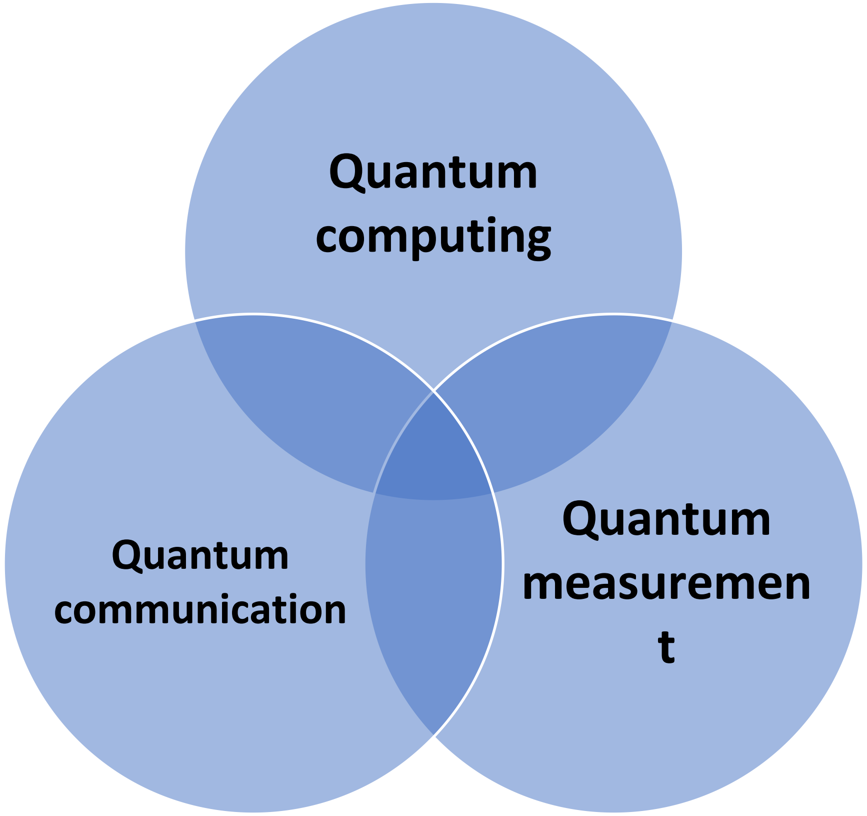
1. Established in 2023, with secretariat hosted by CNIS
2. Responsible for fundamental standards for standard's digitalization
3. Has finished 2 standards for structuring of standard document (GB/T 42093.1 & 2)
4. Is developing 10 standards, covering standard semantic knowledge base, standard-oriented knowledge graphs, standard content modularization, standard machine language, etc.

National Technical Committee for Standardization of Industrial Process Measurement, Control, and Automation (SAC/TC 124)

1. Secretariat hosted by ITEI
2. Responsible for developing standards for industrial process measurement and control
3. Is developing *GB/T Machine Readable Standards Capability Classification Model* (which has entered the final approval stage). This is China's first disclosed model for the classification of machine-readable standards. It differs, to a certain degree, from ISO/IEC's SMART Standards Utility Model.

06

Significance of Quantum Information Technology (QIT)



Main parts of quantum information technology

- Key highlights of the development and industrial upgrading of information and communication technology around the world
- Great influence in future economic development and industrial competition

06

Key SDOs for Quantum Technology

Key Organizations
(besides SAC)

❖China Communications Standards Association (CCSA)

Jinan Institute of Quantum Technology (JIQT)

State Cryptography Administration (SCA)

• China Electronics Standardisation Institute (CESI)

Key TCs for Quantum Technology

National Quantum Computing and Measurement Standardization Technical Committee (SAC/TC578)

- The **only** TC under SAC that is responsible for QIT or even quantum technology
- **Secretariat hosting organization**: Jinan Institute of Quantum Technology (JIQT)
- **Scope**: quantum computing and measurement, mainly involving the standardization terminology and classification, quantum computing and measurement hardware, quantum computing and measurement software, architecture, application platform and other technical fields within the technical scope.

National Communication Standardization Technical Committee (SAC/TC485)

- **Secretariat hosting organization**: CCSA
- **Scope**: the formulation revision of national standards in the fields of communication network, system and equipment performance requirements, communication basic protocols and related test methods.

ST7 of Quantum Communication and Information Technology (CCSA/ST7)

- Founded by CCSA on June 14, 2017, with two WGs:
  - WG1 (Quantum Communication and Information Technology)
  - WG2 (Quantum Information Processing Working Group)

- **Scope:** standardization research on quantum communication and related quantum information processing technologies, to solve relevant standardization problems for the needs of industrial development, and to prospectively layout standard research in new quantum technology

China Standardization Activity in Digital Sector

Features：

- Strong Government plan/led/promotion on standards (like how many standards should be made in which areas in 2024)
- Technology & Innovation supported/feedback to such plans

Challenges:

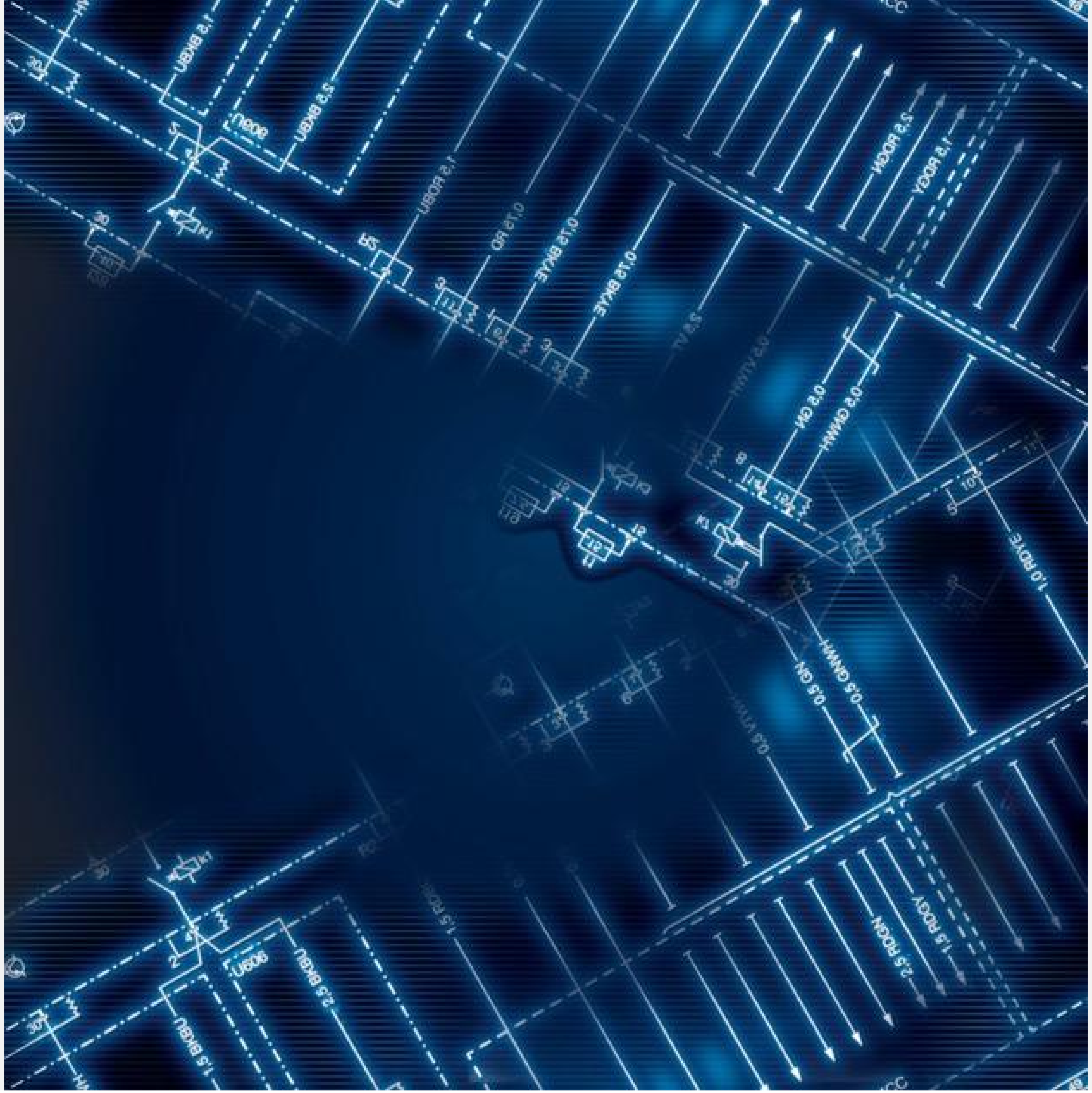
- Balancing innovation and national security
- Fragmentation across sectors

Opportunities/Intentions of China:

- Early-mover advantage in foundation model standards.
- Growing influence in shaping international standards (e.g., ISO/IEC AI standards).
- Leading in emerging tech fields

Trend:

- Continued strong Government plan/led/promotion
- Geopolitical Impact caused segmentation



Thank you!

[Betty Xu] | [April, 2025]