KPMG

Practical guidelines for managing cross-border data transfer in China

July 2022

Key regulatory development of cross-border data transfer assessment

2015 7.1 National Security Law of the People's Republic of China

2017 6.1 Cybersecurity Law of the People's Republic of China

2021 9.1 Data Security Law of the People's Republic of China

2021 11.1 Personal Information Protection Law of the People's Republic of China

2017 4.11 Measures for the Security Assessment of Cross-border Transfers of Personal Information and Key Data (Exposure Draft)

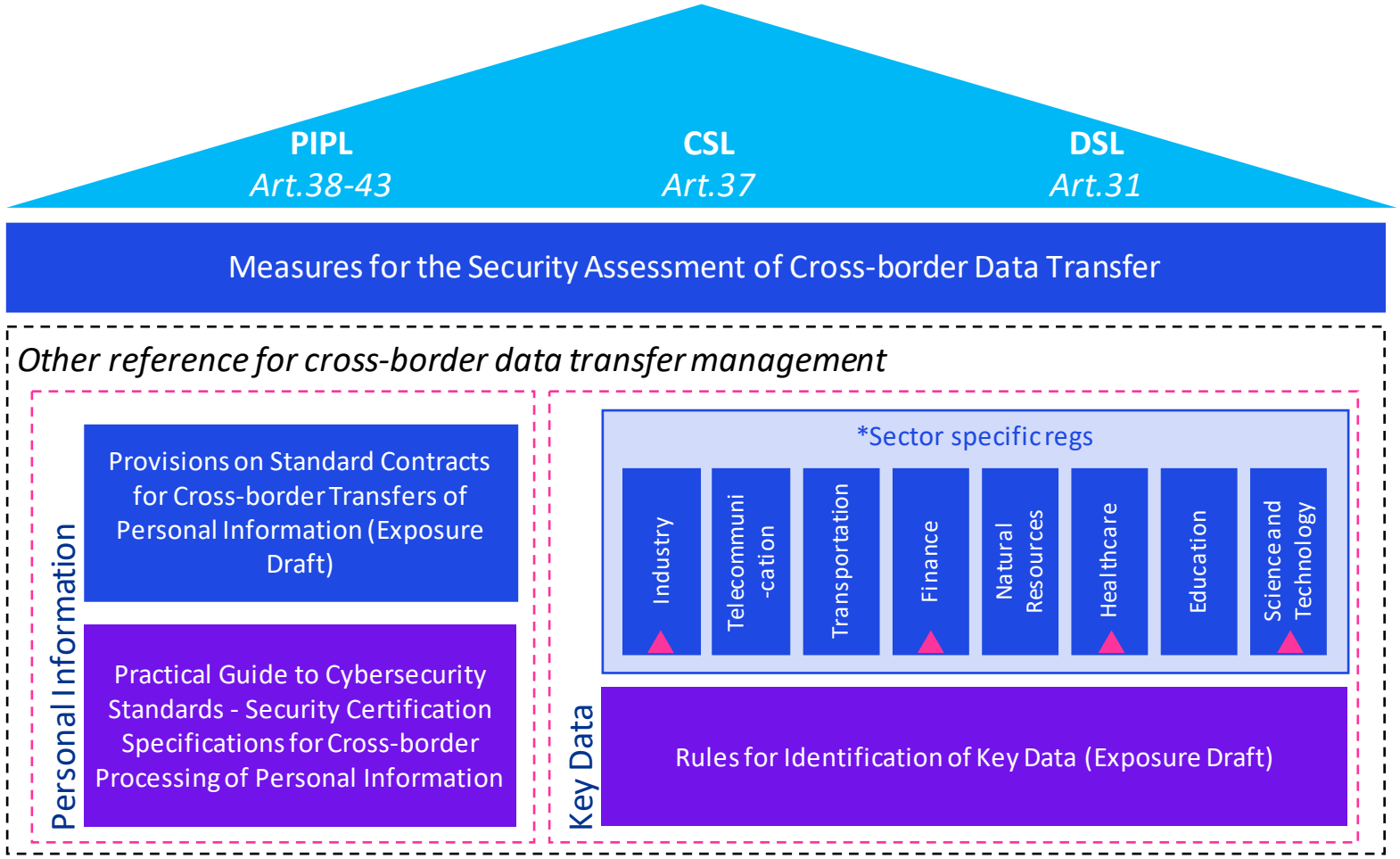
2019 6.13 Measures for the Security Assessment of Cross-border Transfers of Personal Information (Exposure Draft)

2021 10.29 Measures for the Security Assessment of Cross-border Data Transfer (Exposure Draft)

2022 9.1 Measures for the Security Assessment of Cross-border Data Transfer (Enact soon)

"The formulation and promulgation of Measures for the Security Assessment of Cross-border Data Transfer is an important measure to implement the provisions of the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law on cross-border data transfer, with the purpose of further **regulating cross-border data transfer activities**, **protecting personal information rights and interests**, **safeguarding national security and social public interests**, and **promoting the security and freedom in cross-border data transfer**."

Understand the general regulatory framework

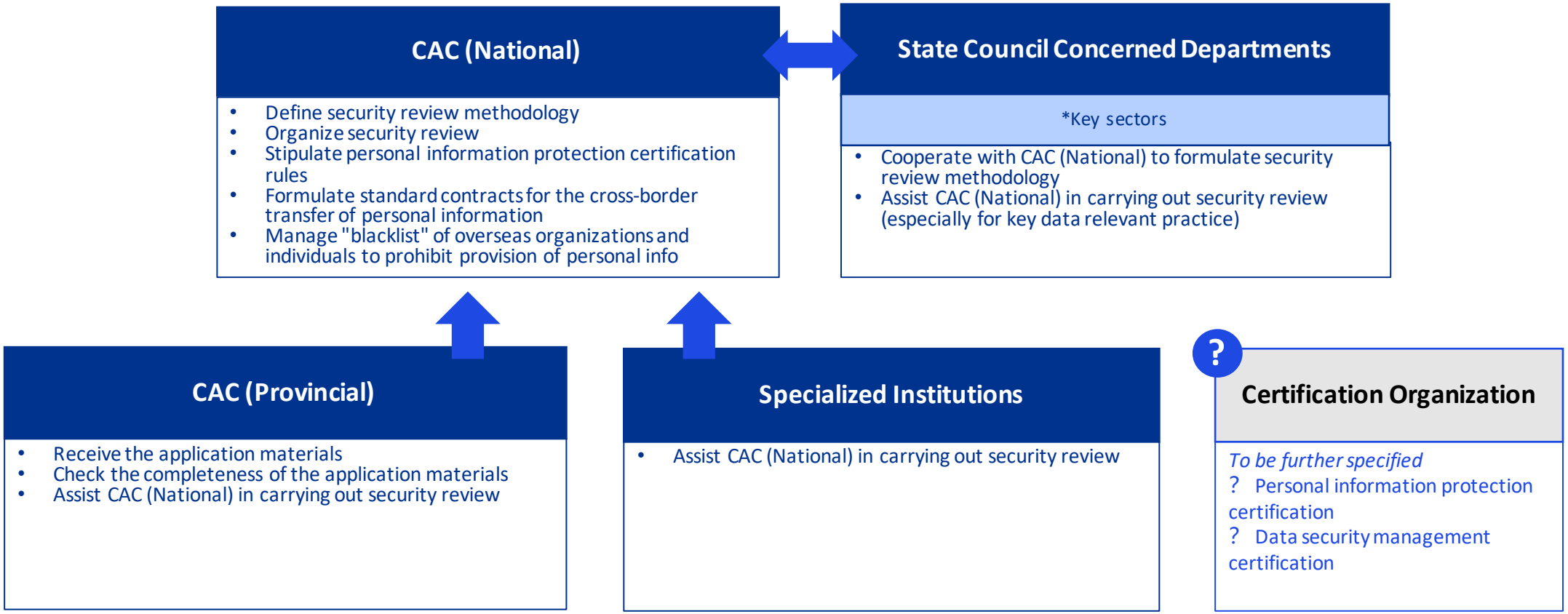


*Administrative Regulations on Cyber Data Security Management (Exposure Draft)

*Industry (Auto): Several Provisions on Automotive Data Security Management (for Trial Implementation)
*Finance: Security Specification of Data Life Cycle
*Healthcare: Guide for Health Data Security
*Science & Technology: Administrative Regulations on Human Genetic Resources

*Personal Information Security Specification
*Guidance for Personal Information Security Impact Assessment
*Cyber-data Process Security Specification (Exposure Draft)
*Guidelines for Data Cross-Border Transfer Security Assessment (Exposure Draft)

Get to know the "external" regulatory organizations in cross-border data transfer management



Recap of "regulated" data

Personal Information

Personal Information

All kinds of information related **to identified or identifiable natural persons** recorded by electronic or other means, excluding the information processed anonymously.

Sensitive Personal Information

The personal information that is likely to result in damage to the **personal dignity** of any natural person or damage to his or her **personal or property safety** once disclosed or illegally used.

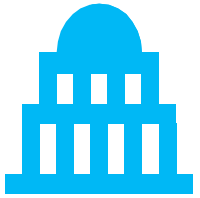
Examples including (the bolded ones are sensitive personal information):

- Name
- Telephone number
- E-mail address
- **Bank account**
- **ID card number or Passport number**
- **Personal health record**
- …

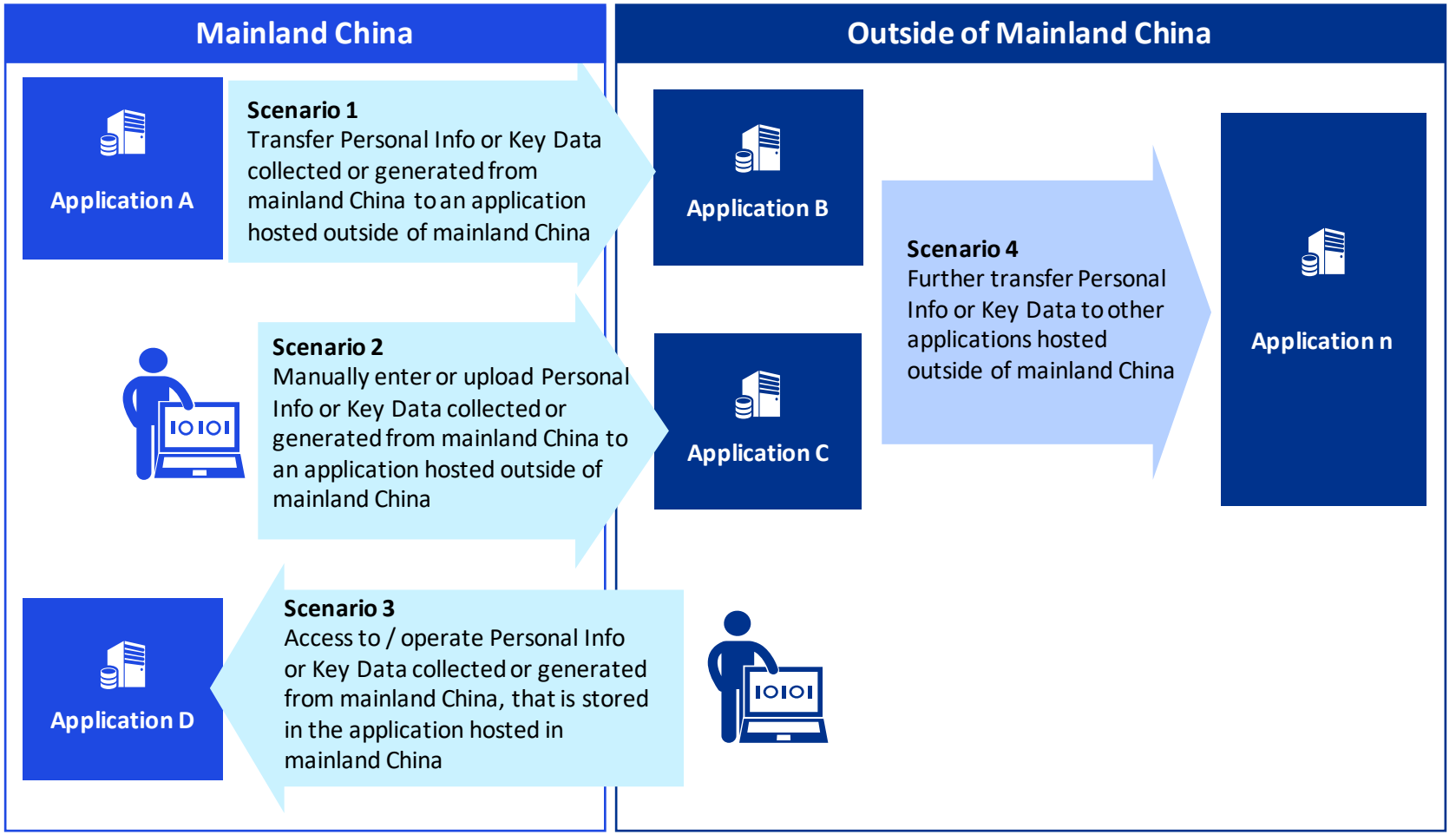
Key Data

Key Data

The data that, once tampered, destroyed, leaked, illegally obtained or used, may endanger **national security, economic operation, social stability, public health and security**, etc., such as undisclosed government information, large-scale population, genetic health, geography and mineral resources, etc.



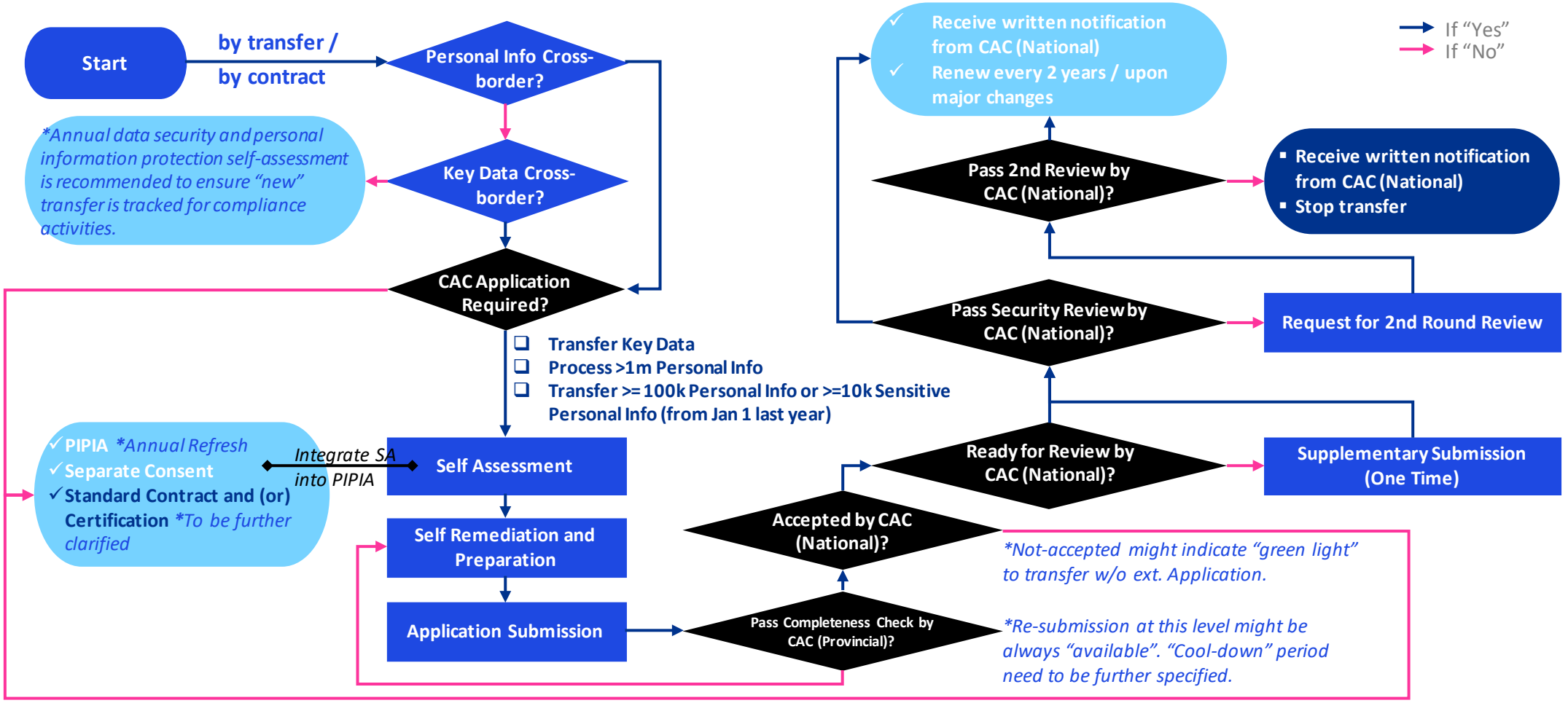
Recap of "cross-border transfer"



Impacted applications

- Business applications with Personal Info and (or) Key Data processed
- IT services and tools which might "contain" Personal Info and (or) Key Data (e.g. logs, backups etc.)
- Third-party services embedded in business applications (e.g. SDKs, PaaS etc.)

Critical path for "network-operator-type" data processor



Self-assessment to get ready with CAC security review

Recommended scope of self-assessment

Processing purpose, scope and approach	*Art.5.1* *Art.8.1*
Impact to lawful rights and interests	*Art.5.2*
Security capability: ❑ Data security risk management during and after cross-border transfer ❑ Protection of data security and personal information rights and interests ❑ Security technology and management capabilities of data receiver	*Art.5.3, 5.4, 5.5* *Art.8.3, 8.4*
Contract compliance	*Art.5.5* *Art.8.5*
Historical compliance	*Art.8.6*
Regulatory and cyber environment of data receiver	*Art.8.2*

Self-assessment report

Data transfer risk	➢ **Data processor (sender) ownership structure** ➢ **Receiver qualification and environment** ➢ **Volume, scope, category, sensitivity** ➢ **Legality, legitimacy and necessity**
Data security risk	➢ **Data processor (sender) cybersecurity capability** **ability to ensure data lifecycle protection* ➢ **Receiver cybersecurity capability** **security management and technical capability*
Contract compliance	➢ **Relevant cross-border data transfer contracts with the overseas recipient or other legally binding documents** (e.g. Standard Contract for Cross-border Transfer of Personal Information)

To be analyzed in CAC security review, better to complete internal analysis during self-assessment phase while information can be provided to CAC (National) when requested.

Contract compliance matters a lot

Take the Provisions on Standard Contracts for Cross-border Transfers of Personal Information (Exposure Draft) as an example:

Obligations of personal information processors (sender)

- Comply with limited purpose and minimal necessary principles
- Implement appropriate notice and consent
- Implement security protection measures
- Receive and cooperate with authority activities, taking joint responsibility of the receiver
- Perform personal information protection impact assessment (PIPIA, 3 years)
- Comply with transparency principle with individual subject (providing data access, copies of contracts, qualification explanation, etc.)
- Conduct contract compliance audit
- Complete standard contract filings

Obligations of overseas recipients (receiver)

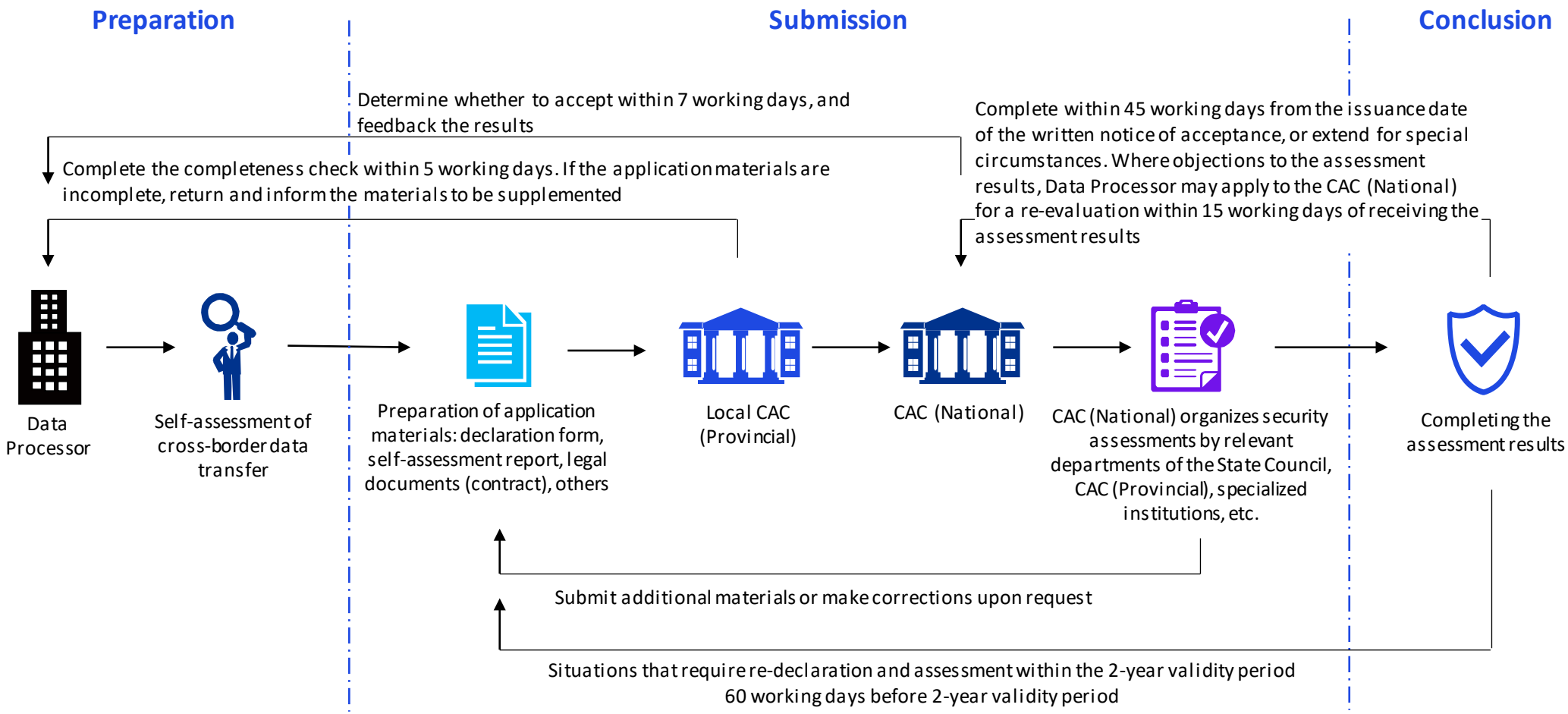
- Comply with limited purpose and minimal necessary principles
- Comply with transparency principle with individual subject (providing data access, copies of contracts, qualification explanation, etc.)
- Strictly enforce data retention policies, conduct disposal audits and provide reports
- Implement security protection measures
- Implement emergency response measures for data breaches
- Carefully entrust further processing or further provide with other 3rd parties
- Comply with automatic decision-making relevant regulatory requirements
- Maintain and retain records of processing activities (RoPA, 3 years)
- Receive and cooperate with authority activities

Personal Info Cross-border Transfer Description

The details of personal information cross-border transfer in accordance with this contract are as follows:
(1) Personal information transferred belongs to the following type of personal information subject(s):
(2) The transfer is for the following purpose(s):
(3) Volume of personal information transferred:
(4) Categories of personal information transferred:
(5) Categories of sensitive personal information transferred:
(6) Personal information transferred is only provided to the following receiver(s):
(7) Transfer approach/mode:
(8) Retention period after transfer:
(9) Storage location after transfer:
(10) Others (where appropriate):

"Data transfer risk" shall be analyzed and summarized based on such description

Timeline for CAC security review



What's next?

2022.07-2022.09

Identify "high-risk" transfer

- transfer that is subject to external application and review

Implement quick-fix

- implement PIPIA, separate consent, standard contract sign-off

Work out Plan B

- define and prepare BCP if "high-risk" transfer is suspended

2022.09-2023.02

Complete self-assessment (pilot)

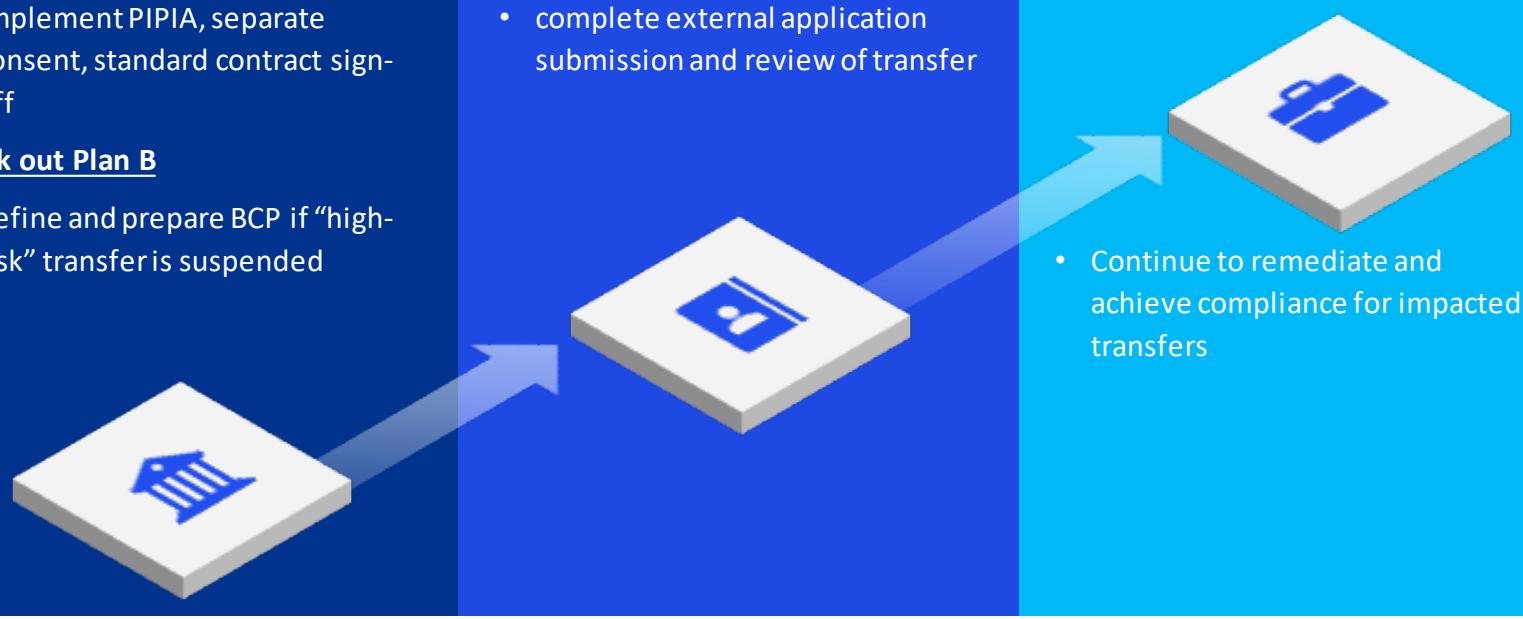
- complete self-assessment and remediation of transfer

Complete external application

- complete external application submission and review of transfer

2023.02 onward

- Establish/upgrade cross-border data transfer management procedure and toolkits, integrate to asset management, data classification and PIPIA processes
- Continue to remediate and achieve compliance for impacted transfers



Keep monitoring

further guidance expected from competent authorities

- Standard Contract for Cross-border Transfer of Personal Info, Legal Documents requirements
- Key Data catalogue of impacted sectors
- Self assessment and security review guidelines and templates
- Enforcement procedure and approach for application submission and communication
- Personal Info Protection Certification guidelines

KPMG services along the journey

Transfer inventory and plan

Identification and inventory of Personal Info / Key Data cross-border transfer and compliance plan for each transfer

Framework design

Cross-border data transfer assessment and management framework and procedure establishment

Self assessment

Self-assessment and remediation

Operational support

Operational support in cross-border data transfer assessment and management

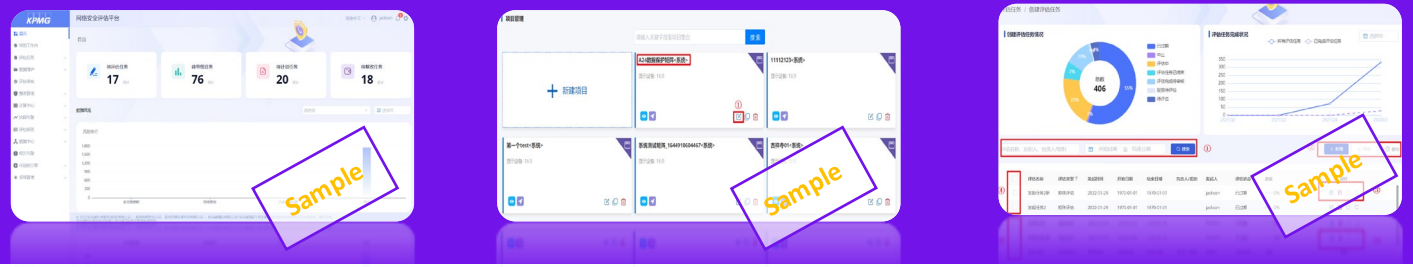
Application and review

Assistance in application submission and security review support

Localization analysis

Analysis and advice on localization strategy and plan

KPMG Cybersecurity Assessment Platform



Contacts

Contact us

Henry Shek
KPMG China
Partner, Cybersecurity

T +852 2143 8799
E henry.shek@kpmg.com

Richard Zhang
KPMG China
Partner, Cybersecurity

T +86 (21) 2212 3637
E richard.zhang@kpmg.com

Danny Hao
KPMG China
Partner, Cybersecurity

T +86 (10) 8508 5498
E danny.hao@kpmg.com

Jason Li
KPMG China
Director, Cybersecurity

T +86 (10) 8508 5397
E jz.li@kpmg.com

Brian Cheung
KPMG China
Partner, Cybersecurity

T +852 2847 5062
E brian.cheung@kpmg.com

Quin Huang
KPMG China
Partner, Cybersecurity

T +86 (21) 2212 2355
E quin.huang@kpmg.com

Kevin Zhou
KPMG China
Director, Cybersecurity

T +86 (21) 2212 3149
E kevin.wt.zhou@kpmg.com

kpmg.com/socialmedia