KPMG

Personal information protection compliance audit management and response

KPMG China

—

March 2025

kpmg.com/cn

Preface

In the digital era, Personal Information (PI) protection has become an important topic in the public's eye and a key compliance obligation for organisations that process personal information. This raises two crucial questions:

- How can organisations ensure that their PI processing activities comply with the regulatory requirements of national laws and regulations?
- How can regulators review and assess the enterprise's personal information protection compliance with data protection regulations?

To address these challenges, a new legislation has been recently introduced to establish personal information protection compliance audits as a fundamental requirement for organisations and provide an institutional framework for conducting them. In China, the Personal Information Protection Law (PIPL) explicitly outlines the compliance audit obligations for personal information processors in Articles 54 and 64. These audits are categorised as self audits and for-cause audits.

To further clarify and guide the implementation of these obligations under the PIPL, the Cyberspace Administration of China (CAC) drafted the Personal Information Protection Compliance Audit Management Measures (PIPCA Management Measures) in August 2023. These Measures were officially released on 14 February 2025 and will come into effect on 1 May 2025.

The Personal Information Protection Compliance Audit Management Measures provide detailed guidance on various aspects, including the scope of application, responsibilities of personal information processors, and other relevant considerations. This comprehensive framework aims to enhance the effectiveness of PI protection compliance audits, thereby encouraging organisations to strengthen their data protection capabilities and implement robust audit processes.

Personal information protection compliance audit management and response

Contents

Background and overview of PIPCA legislation in China

2017.6

The "Cyber Security Law" explicitly proposes the requirements for PI protection in the form of law for the first time

2020

"Information security technology— PI security Specification" (GB/T 35273-2020) puts forward the requirement to conduct "security audits" for PI controllers in the field of personal information protection for the first time in China

2021.12

"Several Suggestions on Promoting Personal Information Protection Compliance Audit" designs a specific personal information audit framework for audit objectives, principles, personnel, contents, procedures, etc.

2021.11

The "Personal Information Protection Law" defines the legal obligation to conduct compliance audit in the field of personal information protection in the form of law for the first time

2023.8

The "Personal Information Protection Compliance Audit Management Measures (Draft for Comments)" and the annex Guidelines are released

2024.7

"Data security technology—Personal Information Protection Compliance Audit Requirements (Draft for Comments)" proposes PI protection compliance audit principles and specifies implementation requirements

2025.2

On February 14, 2025, the "Personal Information Protection Compliance Audit Management Measures" and the annex Guidelines are officially released

2025.1

The "Regulations on Network Data Security Management" proposes that network data processors should conduct compliance audits regularly.

"Personal Information Protection Law of the People's Republic of China"

Article 54: PI processors shall regularly conduct compliance audits of their PI processing activities in accordance with laws and administrative regulations.

Article 64: When the PI protection department of a PI processor finds relatively high risks in PI processing activities or the occurrence of PI security incidents while performing its duties, it may

Consult with the legal representative or the principal person in charge of the PI processor according to the provided authority and procedures.

Request the processor to entrust a professional institution to conduct compliance audits of the personal information processing activities.

"Regulations on Network Data Security Management"

Article 27: A network data processor shall regularly conduct compliance audits, either on its own of by commissioning a professional institution, of its processing of personal information in compliance with laws and administrative regulations.

PIPCA is the basic compliance obligation of all personal information processors

Necessity of carrying out compliance audit:

- **Comply with legislation:** The establishment of the PI protection compliance audit system can improve the PI security legal system, ensure operational compliance with relevant laws and regulations, and avoid fines and legal proceedings;
- **Build trust:** By demonstrating their awareness of PI protection and compliance, organisations can enhance stakeholder trust.
- **Ensure data security:** Compliance audits help identify and reduce security risks, strengthen data security measures, and prevent data leakage;
- **Protect individuals' rights and interests:** Frequent PI compliance audits ensure that enterprises respect individuals' rights and interests, protect personal information security, and avoid to misuse PI;
- **Organise standardised operation:** Guide the organisation to standardise its operations, meet compliance requirements, and improve overall operational efficiency and credibility

According to the PIPL and the PIPCA Management Measures, the compliance audit can be conducted in two ways:

- **Regular self audit:** the PI processor regularly perform self audits on the compliance of its PI processing activities with laws and administrative regulations;
- **For-cause audit:** the regulatory authority responsible of PI protection requires PI processors entrusts professional institutions to conduct compliance audits of their PI processing activities under certain circumstances.

Therefore, enterprises need to establish a self audit system and also consider potential third-party audit possibilities:

Establish Self Audit System

The enterprise conducts audit on a regular basis:

- Processing personal information of more than 10 million individuals: at least once every two years

Self audit can be carried out either internally or by a professional institution.

Responding to Potential For-cause Audits

For-cause audits:

- The PI processing activities present major risks such as serious impact on personal rights and interests or serious lack of security measures;
- PI processing activities may infringe upon the rights and interests of many individuals;
- PI security incidents occur, resulting in the disclosure, tampering, loss, or destruction of the PI of more than 1 million individuals or sensitive personal information of more than 100,000 individuals.

Compulsory audit can only be carried out by professional institutions entrusted by the PI processor, and the personal information processor shall select professional institutions according to the requirements of the protection authorities*, and complete the PI protection compliance audit within a limited time.

*Protection authorities: cyberspace authorities and other authorities performing PI protection responsibilities

Establishing sound personal information protection management is the prerequisite for completing PIPCA

Compliance requirements for PI protection are not "new" requirements arising from the issuance of the Personal Information Protection Compliance Audit Management Measures. Therefore, the basic compliance requirements for PI protection are an important prerequisite for the successful completion of the audit. as：

01

Identify and inventory PI processing activities

- ✓ The type, scope, quantity, and frequency of PI collected, the purpose of collection, the data flow, and the company's role in PI processing
- ✓ The processing records shall be kept according to law

02

Conduct PI protection impact assessment

- ✓ **Circumstances requiring assessment:** A PI protection impact assessment shall be carried out when handling sensitive PI, using automated decision-making to process PI, entrusting to process PI or providing PI to other PI processors, disclosing PI, providing PI overseas, etc
- ✓ **Assessment content:** (a) Whether the purpose and method of PI processing are legal, legitimate, and necessary; (b) Impact on personal rights and security risks; (c) Whether the protective measures taken are legal, effective and compatible with the degree of risk

03

Implement cross-border data transfer (“CBDT”) compliance management

- ✓ **Circumstances requiring CBDT security assessment:** Providing important data overseas; The company is the critical information infrastructure operator; Since January 1 of the current year, it has accumulatively provided PI of more than 1 million individuals (excluding sensitive personal information) or sensitive personal information of more than 10,000 individuals overseas.
- ✓ **Other compliance path: PI protection** certification; Sign a contract with the overseas receiver according to the standard contract formulated by Cyberspace Administration of China (CAC) and file it with the local provincial CAC

04

Improve relevant legal documents for PI protection

- ✓ **PI protection policy or privacy agreement, individual's separate consent:** Except in cases of statutory exemption, the enterprise shall obtain individual consent by agreement before collecting PI.
- ✓ **Standard Contract for Cross-border Transfer of PI:** The contract must be formulated and signed according to the standard contract template provided by CAC.
- ✓ **Data processing agreement:** A personal information processor entrusting the processing of certain personal information to a party, providing personal information for any other processor or jointly processing certain personal information, shall reach an agreement on their respective rights and obligations in processing the personal information.

05

Establish and improve the organisational, management, and technical measures for PI protection

- ✓ Establish a convenient mechanism for individuals to exercise their rights
- ✓ Develop internal management policies and operating procedures
- ✓ Establish an organisation for personal information protection
- ✓ Properly implement PI classification, encryption, de identification and other technical security measures
- ✓ Reasonably determine PI processing scope, and regularly conduct security education and training for employees
- ✓ Develop and organise the implementation of emergency plans for personal information security incidents

PIPCA scope and key domains

While understanding the basics of PI protection compliance is crucial, enterprises should also prepare for compliance audit work in combination with the key points of review suggested in the Personal Information Protection Compliance Audit Management Measures.

Key audit domains of PIPCA

Principles of PI processing activities

- Legality
- Obtaining consent
- Minimum necessary
- Independent choice of multiple business functions

Privacy statement and notice management

- Personal information processing rules / privacy statement
- Notice and consent management

Third parties involved in PI processing activities

- Entrusted PI processing
- Joint PI processing
- Sharing PI with third parties
- Disclosing PI to the public
- Transfer PI in case of merger, division, dissolution and bankruptcy
- Third party management

Special PI processing scenarios

- Processing sensitive PI
- Transferring PI outside of mainland China
- Processing PI with automatic decision making
- Deploying image capturing or personal identification equipment in the public
- Processing publicised PI
- PI processing via APPs

PI protection governance model

- Governance structure and operating model
- Records of PI processing activities
- Privacy compliance management
- Awareness and training management

Privacy management policies and procedures

- PI classification and protection
- Personal information protection impact assessment ('PIPIA')
- PI compliance risk assessment
- Data subject request response
- Data breach incident response
- PI retention policy
- Security engineering for PI protection

Technical measures for PI protection

- Identification and authorisation
- Logging and monitoring
- Data encryption and masking
- Backup and recovery
- Intrusion prevention
- Vulnerability management

Requirements for PI processors in specific situations*

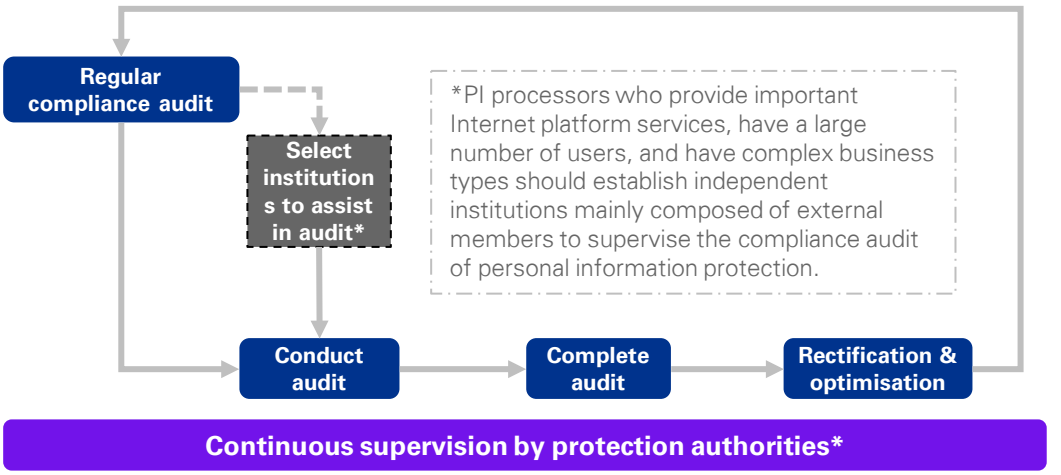
- Platform rule management
- Social responsibility report management

*Includes PI processors who provide important Internet platform services, have a large number of users and complex business types.

Overview of PIPCA process

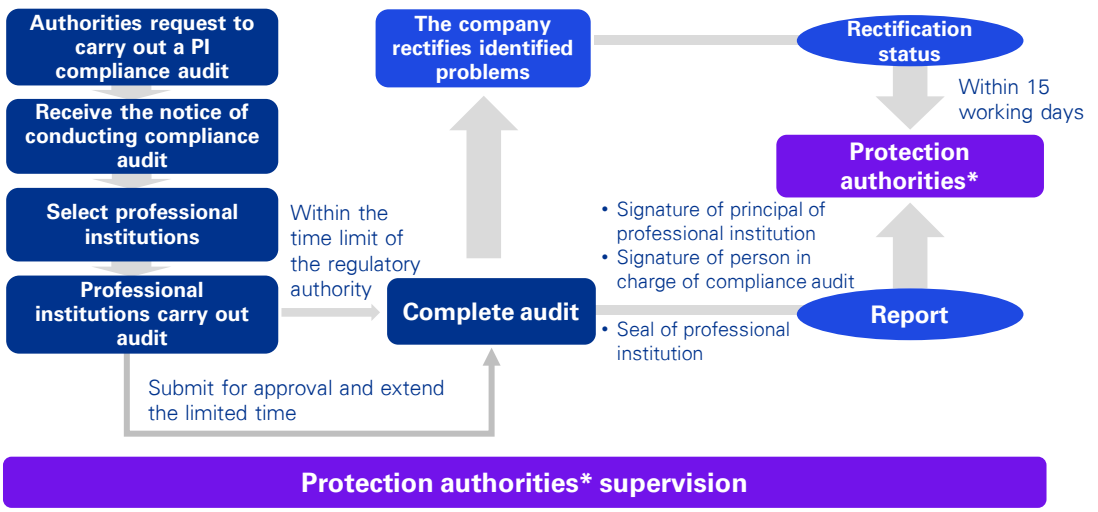
Self audit Process of Personal Information Protection Compliance

Self audit requires PI processors to develop internal audit capabilities, establish corresponding organisational structures, allocate personnel, and define audit methods, audit contents, and audit processes in accordance with the Personal Information Protection Law and the Personal Information Protection Compliance Audit Reference Points.



Regulatory For-Cause Audit Process

Compulsory for-cause audit must be completed by an independent third-party professional institution, including **initiation, execution, reporting, rectification, outcome submission** and other stages.



*Cyberspace authorities and other authorities performing PI protection responsibilities

Recommendations to address PIPCA requirements

The Personal Information Protection Compliance Audit Management Measures provide clear guidance to PI processors on how to conduct compliance audits. The enterprise should establish a PI protection compliance audit policy as soon as possible, defining the specific process and responsible department of compliance audit, institutionalise and systematise the audit strategy, audit method, audit problem rectification, audit result tracking, and other contents, so as to actively respond to compliance supervision, practically improve the maturity of PI management, and support the robustness and fast development of the enterprise. The recommended roadmap of PI protection compliance audit is:

Roadmap of Personal Information Protection Compliance Audit

- **All PI processors should carry out compliance audits on a regular basis (at least once every three years is recommended)**
- **PI processors processing the PI of more than 10 million individuals should conduct a comprehensive audit at least every two years**

Practical guidelines and suggestions for enterprises

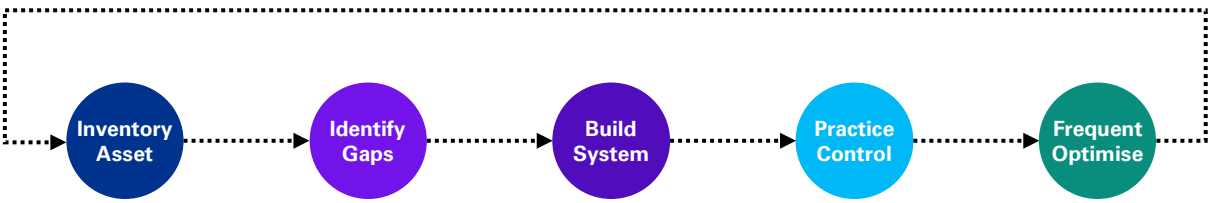
- Establish and improve the company's internal personal information protection compliance audit system, which should be independent from daily compliance management to monitor their implementation and effectiveness.
- Pay attention to the specific requirements of the industry, the specific requirements of the personal information subject, the requirements of special technologies, scenarios, etc., and timely perform the personal information protection compliance audit obligations
- Focus on continuous optimisation and improvement, carry out self-inspection and maturity assessment through regular compliance audit to effectively plan and improve PI protection maturity level.

KPMG personal information protection service

Personal Information Protection Compliance Audit Service

External audit preparation	We provide assistance in preparing for for-cause audits, including but not limited to: assisting in preparing the documents and materials to be audited, assisting in on-site audit performed by the professional institution, assisting in remediation action implementation and preparation of follow-up summaries on remediation action implementation status and results etc..
Internal audit support	According to PIPCA requirements, taking into consideration the current and target state of business and technology operations, we provide support in carrying out regular internal audit, including but not limited to: developing audit policies and procedures, designing audit programme and control matrix, and performing audits etc.
PI protection management optimisation design and implementation	According to PIPL and PIPCA requirements, we provide service in designing PI protection management framework, optimising PI protection management policies and procedures, and enhancing technical measures to truly protect PI and manage the relevant risks.

Overview of the Personal Information Protection Service



Personal information classification and identification & inventory of processing activities	Assessment and planning of personal information protection (governance, process, technology)	Build personal information management framework	CBDT assessment and management framework establishment	Mobile APP/Mini-program privacy compliance assessment and quick rectification
Review and update of privacy policy and relevant legal documentation templates	Personal information protection impact assessment	Design and implementation of security engineering for PI protection (access control, encryption, de-identification, etc.)	Optimisation and audit of third-party personal information protection mgmt. mechanism	Personal information protection maturity assessment or compliance audit

Contact us

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

Danny Hao
KPMG China
Tech Risk
Partner
Tel: +86 (10) 8508 5485
danny.hao@kpmg.com

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

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

Brian Cheung
KPMG China
Tech Risk
Partner
Tel: +852 2847 5026
brian.cheung@kpmg.com

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

Jason He
KPMG China
Tech Risk
Partner
Tel: +86 (755) 2547 3398
jason.rk.he@kpmg.com

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

Jason Song
KPMG China
Tech Risk
Director
Tel: +86 (21) 2212 3306
jason.song@kpmg.com

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

kpmg.com/cn/socialmedia

To obtain information about KPMG offices in China, please scan the QR code or visit our website:
https://home.kpmg/cn/zh/home/about/offices.html