FANGDA PARTNERS
方達津師事務所

China's Final Personal Information Protection Compliance Audit Rules and FAQs

Febuary 18, 2025

NEWSLETTER

The Cyberspace Administration of China ("**CAC**") published the *Measures for the Administration of Personal Information Protection Compliance Audits* (the "**PI Compliance Audit Rules**") on February 14, 2025, which will take effect on May 1, 2025.

The PI Compliance Audit Rules have been in the making for almost two years, since CAC first published the draft rules in August 2023. It is expected that the National Standardization Administration will finalize a national standard on PI compliance audit to flesh out the PI Compliance Audit Rules before May 1, 2025. By then, all regulatory tools would have been set in motion and personal information ("**PI**") handlers (which are similar to data controllers under GDPR) should be prepared for PI compliance audit.

Previously, when it came to comprehensive implementation of Personal Information Protection Law ("**PIPL**"), given the lack of resources and competing compliance priorities, many companies deferred conducting Privacy Impact Assessment ("**PIA**") at the time being and prioritized cross-border data transfer assessment and external-facing matters. With the introduction of the PI Compliance Audit Rules, companies shall pick up these deferred items before the commencement of PI compliance audit. Some matters to be reviewed in the PI compliance audit may be difficult to comply with in practice, such as reviewing the fairness of result in the automatic decision-making process and securing prior approval in the context of sharing data stored in China with foreign authorities and judicial bodies.

Key points of the PI Compliance Audit Rules include:

1. **Territorial Scope:** The rules apply to PI compliance audits conducted within the territory of the People's Republic of China.

   It remains unclear at this stage whether organizations caught by extra-territorial application of the PIPL will also be required to complete the audit in accordance with the PI Compliance Audit Rules. According to the PIPL, Chinese regulators would expect that foreign companies that process China-based individuals' PI shall also use PI compliance audit to ensure its compliance with PIPL.

2. **Audit Requirements:** Organizations must conduct compliance audits either internally or by engaging professional institutions. Organizations that control PI of more than ten million individuals must conduct PI compliance audit at least once every two years.

Organizations that control more than one million individuals' PI shall appoint a PI protection officer (similar to DPO) who should oversee PI compliance audit. This means that DPO of such companies (above one million but at or below ten million) shall set the frequency for PI compliance audit with reference to the prescribed audit in the PI Compliance Audit Rules, such as once every 2 to 3 years. Public oversight and third parties can complain to authorities which may trigger PI compliance audit that is not limited to the prescribed frequency.

3. **Type of Audits:** In addition to carrying out the audit by the organization itself ("**Proactive Audit**"), the CAC and other departments responsible for PI protection can require organizations to engage professional institutions for compliance audits under certain circumstances ("**Reactive Aduit**").

   In a Reactive Aduit, an organization must submit (i) the audit report to the corresponding authority when the ordered audit is completed, and (ii) the rectification report within 15 working days upon the rectification of any issues identified.

4. **Audit Professionals and Institutions:** Professional institutions conducting audits must have the necessary capabilities, including qualified personnel, facilities, and funds. They are encouraged to obtain certification and the certification scheme over institutions and professionals may come later.

   Professional institutions must maintain independence, avoid conflicts of interest, and ensure confidentiality of PI and business secrets obtained during audits. In particular, the same professional institution or same audit responsible person should not serve as auditor of the same company for three consecutive audits.

5. **Supervision and Enforcement:** CAC will supervise compliance audit activities and handle complaints and reports of violations. Violations of the rules will be dealt with according to relevant laws and regulations.

Frequently Asked Questions

Q1: Why does China want to roll out the PI compliance audit scheme?

The reason comes in three folds:

First, corporate liability. Under corporate liability theory, to avoid corporate liability that may implicate an organization and its management personnel, the organization should avoid "window dressing" its policies. An organization will have to actively "police" its policies and leave a track record of evidence. This is where PI compliance audit comes in. Independent auditors should inspect these track records and provide assurance to organization's management that internal policies have been complied with and if not, findings. To the extent engaged, the auditor should monitor how the organization rectify and improve issues identified in the findings. The same is true for privacy. Privacy control points, such as performing PIA should not sit idle, it must be actively performed where required.

Second, law enforcement. Following the promulgation of PIPL on August 20, 2021, China has rolled out many regulations, rules and national standards on privacy protection, in particular, on cross-border data transfer, mobile APP compliance and algorithm regulation. However, law enforcement has been sporadic. The reason behind is that, as is often true across the world, the authorities sometimes do not have sufficient resources to open an investigation on each and every alleged violation. Therefore, it's in the government's interest to have companies run their self-assessment through PI compliance audit such that when there is an incident, the authority can have a bird eye's view over what's going on by looking at the organization's previous audit reports. The fact that an organization actively performed audits is also a mitigating factor when the government determines liability. This is a common practice across the world. In the US, for example, listed companies will need to run SOC Audits to comply with the Sarbanes-Oxley Act.

Third, market practice. When an organization entrusts its data to another organization, such as a SaaS service provider, it will want to request the audit right to make sure the recipient protects the data in compliance with law. As the SaaS vendor cannot accommodate each and every audit request from its clients, the clients are generally happy with an audit report by a third party, hence, there is a need to standardize PI compliance audit practice. This is similar to PCI-DSS audit performed on merchants that participate in payment networks.

Q2: What is the frequency for PI compliance audit?

Proactive Audit: As mentioned above, an organization that processes more than ten million individuals' data is subject to a biennial audit. Those below this volume threshold are not mentioned in this PI Compliance Audit Rules.

It's worth mentioning that in China, sector regulators can promulgate special rules for data protection for their sector which may include data privacy audit/assessment in different shapes and sizes. For example,

according to the data security rule published by the National Financial Regulation Authority (NFRA), companies in banking and insurance sector are subject to a triennial data security audit that appears to be the equivalent of PI compliance audit in that sector. Although on paper, one cannot equalize these special audits with PI compliance audit, there are a lot of overlapping and it's impractical for an organization to perform multiple audits for the same purpose. Avoiding duplicative compliance is also a requirement under Article 52 of Network Data Security Management Measures promulgated by the State Council on September 24, 2024.

Reactive Audit: In addition and separate from proactive audit, the CAC or other authority in charge of PI protection (for example public security bureau) may require an organization to run a PI compliance audit if the organization is found to have potential material data security risk, the organization's data processing activities may infringe on many people's interests, or there is a major data breach that involves more than one million individuals' PI or more than 100,000 individuals' sensitive PI (such as children's information, biometric information, etc.). Reactive audits have no explicit frequency requirement.

To clarify, any organization regardless of the volume of PI processed may be subject to reactive audit.

Q3: How to perform a PI compliance audit? How long does it take?

We see PI compliance audit as a three-step process.

- It starts with **audit preparation**, when the audit scope, audit team, and audit procedure should be developed and put into an audit plan. Most importantly, to maintain audit independence, the auditor should set out audit expectations for each control points and put them into the audit plan. If audit expectations are not articulated, it will create problems and uncertainties down the road which can come back to hurt audit independence.

- Once the audit plan is agreed on, the auditor can go on-site to **perform the audit**. The process is about collecting audit evidence based on an audit checklist, evaluating the condition against criteria to determine if there is potential finding, then validating potential finding to confirm it as a finding. If there is no potential finding or potential finding proves to be false positive, the auditor should provide assurance.

- After the audit is fully performed, the auditor should **prepare the audit report** and material finding list for the management. Depending on the scope of engagement, the auditor may stay on for advisory and monitoring.

In our experience, after the audit plan is agreed upon, the audit process takes two to three months to complete, subject to the complexity of audited PI processing activities as well as the level of cooperation received from relevant stakeholders.

Q4: Is it possible to include PI compliance audit as part of the routine internal audit?

Elements of a PI compliance audit can be included as part of the routine internal audit or self-assessment. Internal audit can also provide assurance. The value position is (1) it helps improve compliance maturity; and (2) it increases readiness for external audit.

However, as a practical matter, internal auditors are not privacy professionals - they may lack knowledge and expertise on data privacy, therefore, the coverage and value of internal audits may not be as sufficient as a special PI compliance audit. Nevertheless, for financial institutions where there is mandatory internal audit, it makes sense to have an internal audit cover PI compliance audit to avoid duplication of efforts.

Q5: Is it possible to include PI compliance audit as part of IT security check-up?

As the saying goes, "privacy can't go without security, but security can stand on its own without privacy." IT security focuses on different aspects of privacy, therefore, relying solely on IT security check-up may not be sufficient. Since the PI Compliance Audit Rules include both privacy control points and security control points, if an organization has existing IT security audit reports, it makes sense to reuse the outcome for the PI compliance audit to cover parts of the control points.

Q6: What's the best way to determine the scope of the audit?

We would recommend companies take a risk-based approach and prioritize the risk items that they care most. The order can flow from business function to channels and then to control points. For example, in China, Apps that in breach of data protection laws may be published on a list and will be ordered to rectify and taken down from the App store. If the company is a consumer-facing organization with substantial digital sales, then it makes sense for the company to focus on special control points on the App.

Q7: How to prioritize audit findings?

The starting point should be the materiality of control points that was agreed under the audit plan. Special consideration should be given to the potential enforcement risks associated with the control points. Lastly, during an audit, it is possible that the organization may not have sufficient resources or time to fully audit in-scope control points, for example, if it requires extensive technical testing. In this case, to avoid compromising the quality of the audit, the organization may create a Phase II audit to fully cover the outstanding control points.

Q8: What are the common findings?

At a high level, the common findings fall into the following categories:

- Governance, such as the appointment of DPO, lack of comprehensive policies; or policies have not been rolled out;
- Full-lifecycle data protection. Most findings are about third-party data sharing, response to data subject rights and data retention, etc.; and
- Specific control points, such as PIA, record of processing activities (ROPA), incident response plan (IRP), etc.

Q9: How to communicate the findings and recommendations with the management?

After the management's deliberation and buy-in of the findings, an organization can ask for a budget to start projects to cure the most important findings following advice from the auditor. In this process, the organization can engage auditors to play a monitor role.

In practice, the management may expect to tag a dollar value to each finding. However, it may not be practical in China as there is no detailed dollar amount for the penalty for each kind of violation, except for the general penalty set at RMB 50 million or 5% turnover under the PIPL. Besides, the damages in civil litigations are inconsistent and may require systematic monitoring of judicial practice. In this regard, monitoring the authorities' enforcement priority is critical in helping the management understand the implications of the findings.

Q10: Why is PIA front and center to PI compliance audit?

In our experience, PI compliance audit with respect to a specific control point can follow a three-step approach, (1) mapping out business flow, (2) understanding data flow, and (3) completing gap assessment. In this process, ROPA can be a first step and comparing ROPA against control points in organization's policies follows. Since this step overlaps with PIA, if the organization already has PIA result, the auditor will be focusing on the result. If not, the absence of PIA is likely to constitute a potential finding on its own and it also increases the auditor's audit cost because it will have to start from scratch.

Beijing
27/F, North Tower
Beijing Kerry Centre
1 Guanghua Road
Chaoyang District
Beijing 100020, China
Tel: +86 10 5769 5600
Fax: +86 10 5769 5788

Guangzhou
66/F, Guangzhou CTF
Finance Centre
6 Zhujiang East Road
Zhujiang New Town
Guangzhou 510623, China
Tel: +86 20 3225 3888
Fax: +86 20 3225 3899

Hong Kong
26/F, One Exchange Square
8 Connaught Place, Central
Hong Kong
Tel: +852 3976 8888
Fax: +852 2110 4285

Nanjing
38/F, Asia Pacific Business Building
2 Hanzhong Road
Gulou District
Nanjing 210005, China
Tel: +86 25 8690 9999
Fax: +86 25 8690 9099

Shanghai
24/F, HKRI Centre Two,
HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041, China
Tel: +86 21 2208 1166
Fax: +86 21 5298 5599

Shenzhen
9/F, Tower One, Kerry Plaza
1 Zhong Xin Si Road
Futian District
Shenzhen 518048, China
Tel: +86 755 8159 3999
Fax: +86 755 8159 3900

Singapore
1 Raffles Place #55-00
One Raffles Place Tower 1
Singapore 048616
Tel: +65 6859 6789
Fax: +65 6358 2345