AVISTA INSIGHT

Highlights of the Compliance Audit Requirement in the “Administrative Measures for the Personal Information Protection Compliance Audit (Comment Draft)”

Preface

On August 3, 2023, to guide and regulate the compliance audit activities of personal information protection, pursuant to the "Personal Information Protection Law of the People's Republic of China" (hereinafter referred to as the "**PIPL**") and other relevant laws and regulations, the Cyberspace Administration of China issued "Administrative Measures for the Personal Information Protection Compliance Audit (Comment Draft)” (hereinafter referred to as "**Management Measures**") and the annex of "Reference Points for Compliance Audit of Personal Information Protection" (hereinafter referred to as "**Reference Points**") for public comments.

The Management Measures and Reference Points are provided to further enhance personal information protection regulations and corporate internal compliance systems in China by clarifying the requirements and forms of personal information protection-related compliance audit (hereinafter referred to as “**Compliance Audit**”).

Through highlighting some key provisions in the Management Measures and Reference Points, this article is providing readers a more intuitive understanding of the requirements in the Compliance Audit and providing advices for personal information processing enterprises how to conduct the Compliance Audit in accordance with the applicable laws and regulations.

What is personal information protection compliance audit?

As mentioned in the Management Measures, the Compliance Audit is defined as a supervisory activity that reviews and evaluates whether the personal information processing activities of personal information processors comply with applicable personal information protection-related laws and regulations.

The Compliance Audit should clearly define the types of personal information to be audited, which include general personal information and sensitive personal information.

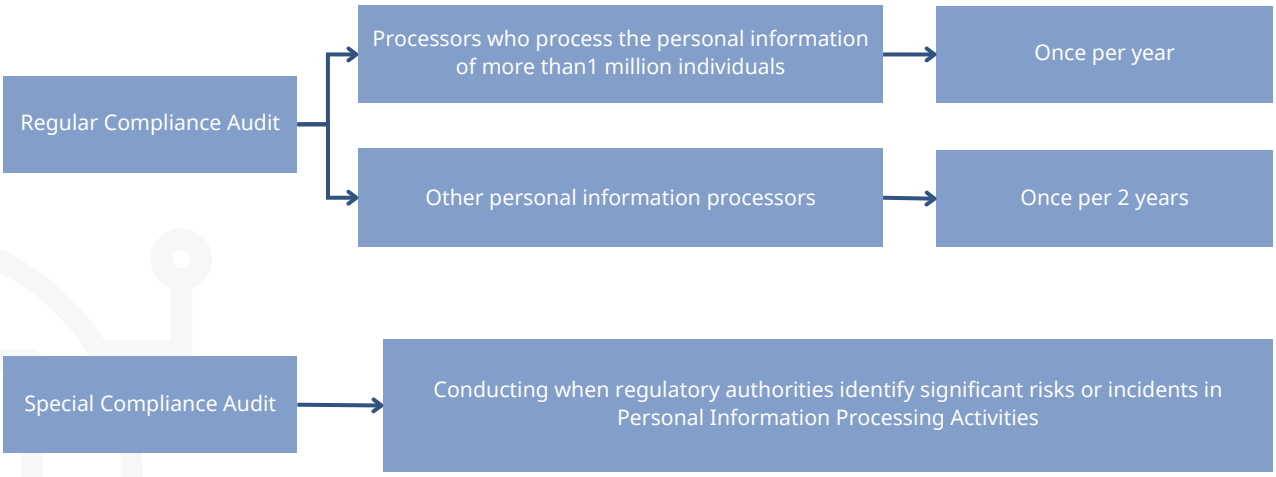
General Personal Information	Personal basic information, general identification information, online identity information, personal education and work information, personal communication information, contact information, personal internet usage records, commonly used personal device information, personal location information, and other information.
Sensitive Personal Information	Biometric information, religious beliefs, specific identity, medical and health information, financial accounts, whereabouts and tracks, and personal information of minors under the age of fourteen.

Why conduct the Compliance Audit?

Article 54 and Article 64 of the PIPL stipulate the legal obligations of "regular compliance audits" and "special compliance audits". Any company failed to fulfill its obligations to conduct compliance audits will be subject to punishment in accordance with Article 66 of the PIPL, including confiscation of illegal proceeds, suspension of business, fines, and revocation of business qualifications.

Who should conduct Compliance Audit?

Articles 4 and 6 of the "Management Measures" detail the criteria and categorise the Compliance Audit, as required in PIPL, into "regular compliance audits" and "special compliance audits", which has been summarised as follows:



Who is the appropriate person to conduct the Compliance Audit?

1) Audit agencies

Articles 5 and 7 of the Management Measures defines the appropriate person as below:

Compliance Audit Types	Main Body
Regular compliance audit	Internal structure of the organization or external professional agencies
Special compliance audit	External professional agencies

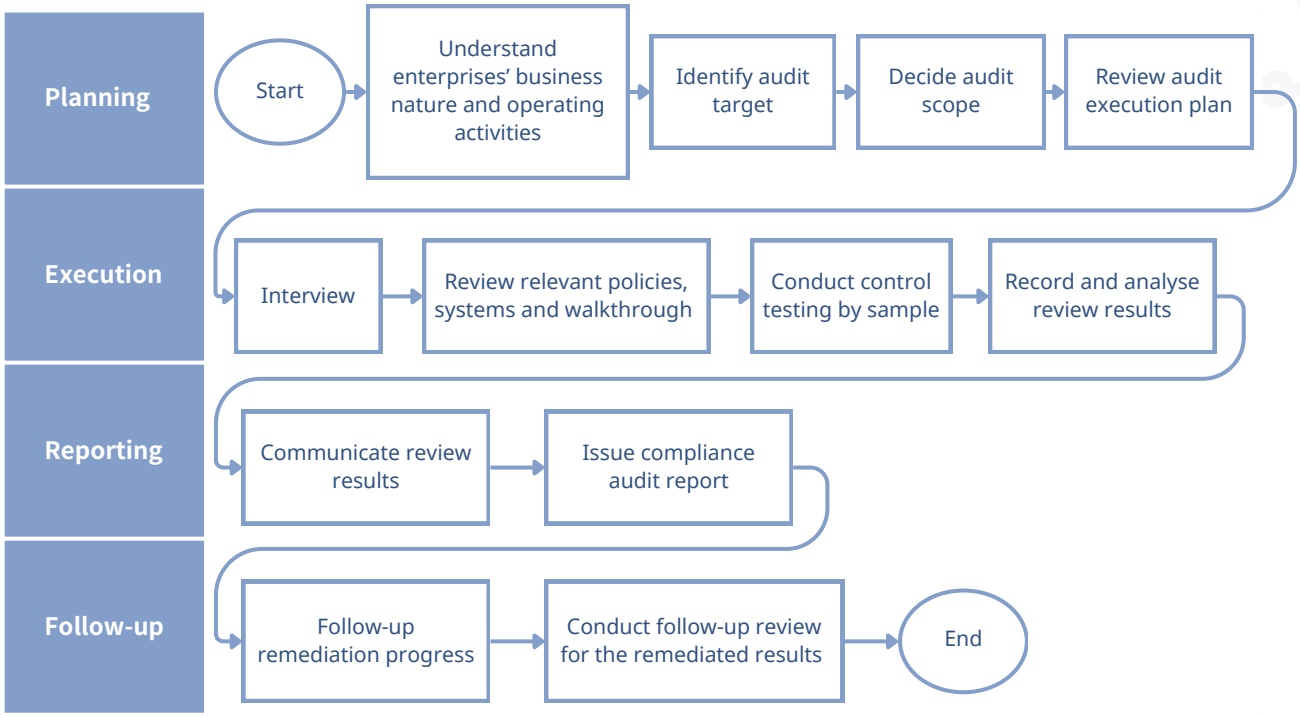
2) Audit approach comparison

3) Requirement for professional agencies

Pursuant to the Management Measures and Reference Points, to ensure the objectivity of the Compliance Audit, professional agencies should not perform the Compliance Audit for the same entities more than three consecutive years.

Except for some enterprises requiring official verification in information security capabilities and technical measures capability, the major focus for the Compliance Audit are risk evaluation and review of internal control systems. Therefore, enterprises can choose consulting agencies expertise in internal control review and consulting with considerable experiences in risk and compliance advisory industry.

What are the work processes of the Compliance audit?



What are the key focuses of the Compliance Audit?

1) Key policies and systems

We have summarized some key policies and systems to be focused in the Compliance Audit, as follows but not limited to:

- Strategies, objectives and principles
- Duties and responsibilities
- Data classification & management
- Emergency plan
- Impact assessment and compliance audit policies
- Complaint management
- Training and continuous education
- Staff performance evaluation
- Non-compliance management

2）Audit focuses for different industries

- **Financing and money-lending**

Audit Focus	Key Points
Collection and use of real-name information	When enterprises collects sensitive information such as loan applicants' identity and contact information, transactions, and consumption details, do they obtain a clear consent from the applicants? In addition, does the enterprises excessively collect applicants' personal information?
Security technical measures	What security measures have the enterprises taken for confidentiality and integrity protection of personal data? Is there any encryption in data transmission and storage for security purpose? Are there measures to prevent unauthorized access?
Communication information security	Does the enterprises use personal information not in accordance with applicable laws and regulations for repayment collection using text messages, emails, and phone calls? In addition, does the enterprises protect loan applicants' personal information from threats such as cyber attacks and telecommunications fraud?
Emergency response mechanisms	Has the enterprises established a holistic emergency mechanism to respond effectively to personal information security incidents in a timely manner?

- **Online platform service**

Audit Focus	Key Points
Registration and user data collection	For the personal information collected during platform user account registration, have the enterprises clearly informed users for the purpose and approach of data collection and obtained their consent?
Data storage and cross-border transmission	For enterprises planning to be listed outside China and involving in cross-border data transmission, have they obtained appropriate official authorization following the requirement in the relevant laws and regulations? Have necessary security measures been taken to secure personal information in data storage and during cross-border transmission?
Transaction data and payment information	Have the enterprises taken sufficient security measures on users' payment information and transaction data? In addition, enterprises need to consider if the data processing procedures aligns with regulatory requirements to avoid abuse or improper use of those data.
Personalized recommendations and advertising	For leveraging users' social relationships, browsing preferences to formulate personalized recommendations and advertisements, during compliance audit, transparency assessment on users notification and consent of such behavior should be considered. In addition, users should be able to choose, without excessive restriction, whether to accept those personalized recommendations.
Personal information protection impact assessment	Have the enterprises conducted a personal information protection impact assessment to determine the potential impact of data processing activities on user rights and benefits and taken corresponding measures to reduce these impacts?
Social responsibility report	Do the enterprises regularly publish any social responsibility reports to transparently disclose the protection mechanism for personal information to stakeholders?

- **Retail**

Audit Focus	Key Points
Consumer member information collection	When collecting consumer membership information, have the enterprises discharge its legal obligation by informing consumers the intended use of the collected personal information? In addition, has the collected personal information been encrypted to prevent unauthorized access by employees?
Third-party cooperation and data sharing	For data sharing activities with different third party platforms rendering services for goods transportation and delivery, membership management, and QR code payment portal, in the service agreement entered with those third party platforms, are the personal information data security approaches and measures clearly written?
Compliance education and training	Have the enterprises provided compliance training for employees to enhance their awareness and capability in personal information protection?

Conclusion

The Management Measures provides clear guidance on how enterprises should conduct the Compliance Audit. Enterprises should be aware of the importance the Compliance Audit and consider it as a tool to identify and manage potential risks in personal information processing activities, ensuring that the enterprises operate in compliance with the applicable laws and regulations.

Avista Risk Advisory is aware of the rapid development of the laws and regulations in personal information protection in recent years. By leveraging our deep understanding in the regulatory requirements in personal information protection, Avista can provide enterprises with professional, comprehensive and practical solutions in relation to the Compliance Audit as well as personal information protection governance enhancement to align with the latest regulatory requirements.

Contact Us

Vincent Pang
CFA, FCPA, FCPA (Aust.), MRICS, RICS Registered Valuer

Managing Partner
vincent.pang@avaval.com
+852 3702 7388
+86 138 1023 8603

Derek Chim
CPA

Principal
derek.chim@avaval.com
+852 3702 7312
+86 189 3866 2083

Website Facebook LinkedIn WeChat

AVISTA Group ("AVISTA") is a leading professional advisory firm. We are experienced in performing a full range of Valuation Advisory, Risk Management Advisory, ESG Advisory, Corporate Advisory, and Property Consultancy services for various purposes. AVISTA is a corporate member of The International Valuation Standards Council (IVSC).

With a strong presence in the Asia-Pacific region, we have offices in Hong Kong, Shanghai, Beijing and Shenzhen. Through effective utilization of our local and international networks and the synergies among our service lines, we aim at providing high-quality services to clients and assisting clients in formulating strategies to maximize their value under complex business circumstances.

The AVISTA professional team comprises more than 100 professional consultants, each with different areas of expertise and detailed familiarity of financial reporting standards and regulatory standards. Our team of experienced professionals come from globally-renowned valuation firms, consulting firms and international accounting firms with global qualifications such as CFA, CPA, CPV, FRM, MRICS, FCCA and so on.