PING AN
Expertise Creates Value

Expertise Makes Life Easier

Policy Statement on Information Security of Ping An Group

March, 2024

As Ping An Group advances its comprehensive digital transformation, the digital business landscape becomes increasingly diverse, and the volume of real business data is growing rapidly. With this evolving landscape, information security has become a crucial cornerstone for Ping An to achieve sustainable development. Ping An commits to managing information security risks with high standards to ensure the secure and reliable operation of the information systems across the entire Group. This commitment provides a solid foundation for offering diverse products and convenient services to customers in all business sectors.

Scope of Application

This policy statement applies to Ping An Group, all member companies, departments, employees, and third-party individuals who have access to information assets, including but not limited to personnel from outsourcing companies, agents, vendor engineers, consulting company advisors, and others. This policy covers all business sectors of Ping An.

Commitment

Ping An commits to conducting information security management at high standards, which includes:

- Abide by the highest information security standards in accordance with respective laws, regulations, and industry standards and codes;
- Provide sound information protection to ensure information confidentiality, integrity and accessibility;
- Build information and information security controls systems based on Defense in Depth (DiD) and Secure by Default standards;
- Protect information and information systems according to its sensitivity, value, and importance.

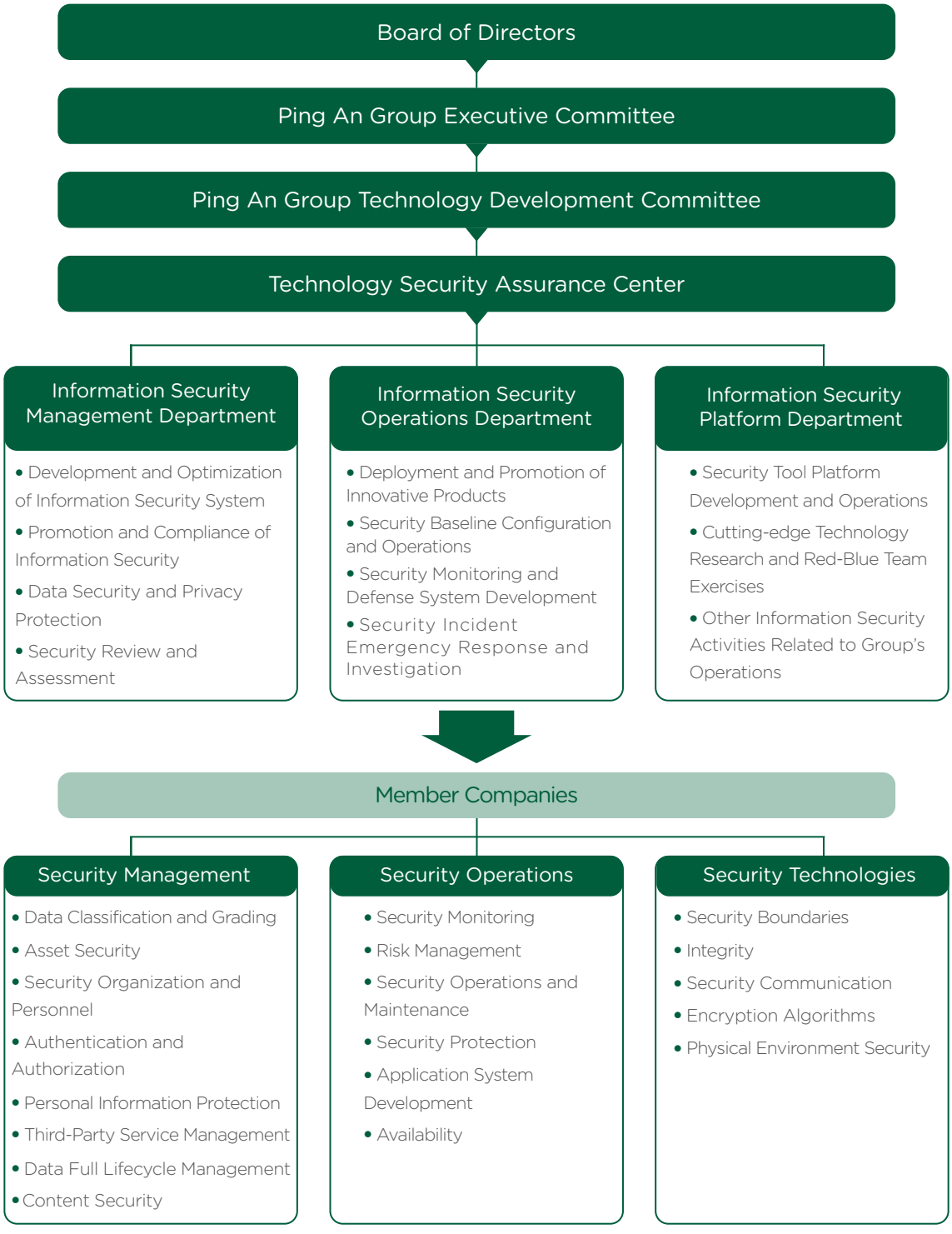
Information Security Management Framework

The Board of Directors is responsible for supervising the management performance of the Group's information security, as well as supervising, evaluating and ensuring the effectiveness of the information security management system, and assuming ultimately accountable for the Group's information security risk management. The Group's Technology Development Committee (referred to as the Technology Committee) is the leading body for information security in the Group, overseeing the effective and continuous execution of information security management measures in the Group. The Security Assurance Center, under the Technology Committee, coordinates the work of network security, data security, and personal information protection primarily at the Group level.

It is responsible for coordinating, planning, building, promoting, and organizing information security work.

Each member company has designated personnel responsible for network security, data security, and personal information protection, ensuring the fulfillment of their respective responsibilities. They implement specific control strategies to ensure data confidentiality, integrity, and availability.

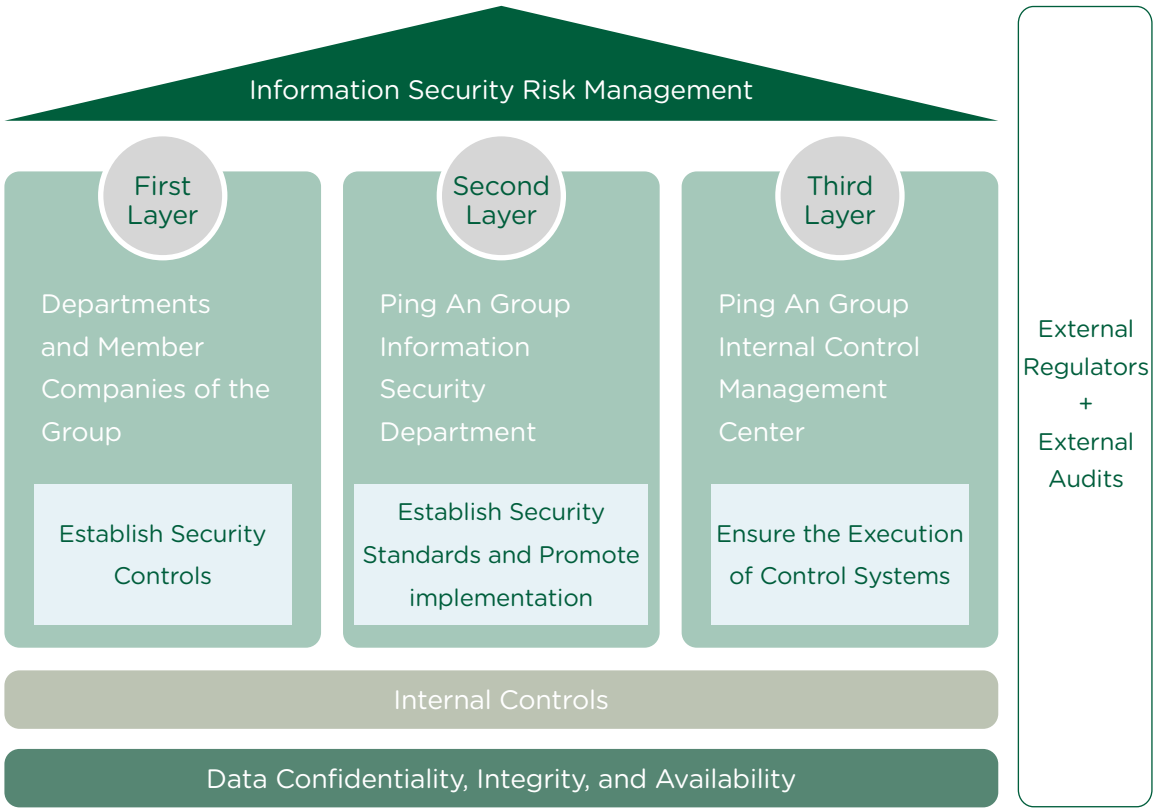
The Ping An information security management framework and its main scope of work are outlined as follows.



Information Security Management System

Information security risk management is a coordinated set of activities that guide and control the impact of information security risks on the company. This includes tasks such as assessment preparation, risk identification, risk classification, risk evaluation, risk analysis, risk mitigation, risk monitoring, risk approval, risk reporting. The primary objective is to thoroughly identify and assess information security risks, ensuring that these risks are comprehensively identified and kept within acceptable limits to reduce their impact on the organization.

Ping An's information security management system consists of three lines of defense, each with different information security roles and responsibilities. Every member of Ping An takes a collective responsibility to protect information assets.



First line of Defense

The first layer encompasses various departments and member companies within the Group. Their primary responsibility is security control, which involves the establishment of security controls, incident response, and remediation measures to safeguard the confidentiality, integrity, and availability of information asset.

Second Line of Defense

The second layer involves the Group's Information Security Department. Its main role is to develop security standards and promote their implementation. This is accompanied by implementing an information security system, conducting compliance reviews, assessing training programs, and enhancing information security management practices.

Third Line of Defense

The third layer is managed by the Group's Internal Control Management Center. Its main responsibility is to ensure the execution of control systems. It conducts independent reviews and assessments of information security activities in various departments and member companies within the Group.

Information Security Principles and Measures

Ping An has formulated information security management principles and measures based on laws, regulations, and industry standards. These are focused on security management, security operations, and security technology and consist of 12 key categories:

Asset Security and Data Classification and Grading

• All information assets, including but not limited to written, oral, and electronic information, should be classified and identified based on their sensitivity, importance, and access restrictions required by business needs.

• All important assets related to information should be marked on the assets list, which is maintained and updated on a timely basis.

• Data should be classified and graded according to data classification principles and rules, with different levels of confidentiality protection requirements assigned to different data categories.

Security Organization and Personnel

• All job descriptions must include a description of information safety responsibilities and indicate the sensitivity of the information involved.

• Employees must pass ethical integrity assessment and sign a confidentiality agreement before coming on board. Relevant procedures must be followed to ensure the protection of information assets when staff changes position or leaves the company.

• Individuals who violate Ping An's information security policies will be subject to penalties according to the latest Red, Yellow, Blue Card Penalty System. And for serious violations, Ping An may pursue legal action.

• To raise awareness of information security, all new employees are required to complete information security training during the first three months of their employment. In addition, Ping An conducts annual information security training for all employees and third-party personnel, covering areas such as data security, personal information protection, and terminal security. This comprehensive training aims to enhance employee awareness and skills related to information security. Meanwhile, all member companies provide targeted business information security training in line with business practices under the Group's guidance.

Authentication and Authorization

Accountability

Users need to be authenticated before accessing information and information systems. The authentication method is compatible with the sensitivity and risk of the information.

Authorization

Users are to follow the minimization and need-to-know principles and are only permitted to access necessary information.

Responsibilities

A single person cannot handle the entire business transaction or operating procedure on their own. High-risk functions must take effective monitoring measures, including process splitting, process rotation, enforcement checks and other approval procedures.

System Development and Maintenance

- Implementation of security regulations should be strictly followed during application development, release, and updates. E-commerce applications should be designed to protect the confidentiality and integrity of customer information in the public network environment and ensure the non-repudiation of the transaction.

- The encryption algorithm used must meet the principles of data protection, including achieving the confidentiality, integrity, authentication, and non-repudiation and has been publicly verified. The encryption key must be properly managed throughout the key life cycle.

- Adopt strong identity authentication methods such as two-factor authentication for important systems, and grant access strictly following the "least access, need-to-know" principle to prevent internal data theft. At the same time, advanced technology is used to strengthen system log auditing, and track and identify data leakage.

- During operations and maintenance, it is essential to ensure the execution of relevant change processes to prevent unauthorized malicious or accidental alterations or deletions of information.

Security Monitoring and Protection

• Ping An employs a combination of proactive and passive defense measures to maintain system information security. It monitors and records information activities and manages the entire process of information security incidents, ensuring that all significant accesses and operations within Ping An's information systems are recorded. This guarantees traceability of sensitive activities within the system, allowing for precise attribution to responsible individuals. Furthermore, Ping An responds to and manages information security incidents in a timely manner to ensure the safety and stability of information assets, data, and all business operations.

• In terms of network intrusion, Ping An deploys network security devices such as DDoS, IPS, and WAF according to the network security risk situation. It also deploys security platforms/tools like APT situational awareness defense systems and honeypot systems to provide comprehensive security monitoring, analysis, warning, and response.

• Regarding threat intelligence, Ping An establishes a security emergency response platform and implements threat intelligence systems. It collects information related to threats to information security, conducts analysis and investigation, issues security warnings, and tracks the progress of remediation.

Regional Boundaries and Communication Security

• Ping An deploys appropriate access control mechanisms at network boundaries based on different network zones and establishes access control rules.

• Ping An monitors network performance, traffic, and unauthorized access, and promptly addresses or reports any anomalies.

• Ping An implements proper security measures to prevent malicious or accidental unauthorized alteration or deletion of information assets.

• All connections to Ping An's network must incorporate appropriate security measures to protect internal networks, information, and information systems, especially for connections to public networks and networks not managed by Ping An.

• Major networks and operating systems should receive important patches within an appropriate timeframe, and newly built operating systems should be configured with the latest patches.

• All servers, workstations, and relevant devices must be equipped with antivirus and anti-spyware software. Ping An routinely updates and upgrades the antivirus system and virus libraries to prevent malicious code attacks.

Business Continuity Planning

• Ping An has established appropriate measures to ensure that information is available to authorized users. In the case that the original data is destroyed or lost, the most recent backup information is extracted to achieve continuity of the service.

Information Security Compliance

• Ping An protects customer information and privacy, and strictly follows information security requirements in accordance with the highest standards in laws, regulations, and contractual requirements.

• Ping An complies with obligations such as classification protection, protection of critical information infrastructure, security evaluations of commercial cryptography applications, and network security reviews.

• Websites, apps, mini-programs, quick apps, and other online services must apply for domain registration or permits for internet information services from regulatory authorities as required by law. The registration number or telecommunication business operation permit number should be prominently displayed on the website's homepage or in the app.

Information Security Audit and Certification

• Ping An conducts internal audits of its information security management system at least once a year, with audit results reported to the Group's Board of Directors, Executive Committee, and Risk Management Committee.

• Independent external audits of information security are conducted at least once a year and specific audits and inspections are carried out in accordance with regulatory authorities' management regulations and requirements.

• Ping An actively promotes certification for information security management system standards applicable to business operations, including but not limited to ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and others.

Supplier and Third-Party Information Security Management

• Ping An upholds stringent standards when it comes to managing the information security of supplier and third-party service. Suppliers refer to legal market entities or other organizations that directly or indirectly provide products or services for Ping An within the procurement business. Third-party service personnel include but are not limited to personnel from outsourcing companies, agents, vendor engineers, consulting company advisors, and more. With the core principle of "sensitive data stays within Ping An", Ping An formulates and implements management systems such as the Group's Third-Party Service Security Management Standard and Supplier Information Security Management System in accordance with relevant laws and regulations, taking into account the actual business situation. Ping An implements procurement management, classification and grading, contract terms, monitoring and evaluation, risk management, regulatory reporting, and other management requirements. Through effective communication, Ping An ensures that suppliers and third parties are well-informed of and comply with Ping An's management requirements, effectively reducing information security risks associated with supplier and third-party cooperation.

• Ping An regularly assesses the compliance of cooperating suppliers and third parties in terms of information security and privacy protection, including but not limited to data storage, management systems, technical measures, access control, disaster recovery facilities, and emergency management systems. Additionally, Ping An conducts due diligence on important suppliers through questionnaires and other methods, and conducts on-site audits as needed.

Content Security

• Ping An establishes an information content security review management mechanism, following the principle of "review before publication". This involves actively filtering and monitoring content to identify and proactively block illegal and undesirable content to ensure the legality, accuracy, and authenticity of information and maintain a healthy online environment.

Physical and Environmental Safety

• Ping An has adopted strict physical security precautions to prevent information from unauthorized access, destruction, and interference. In preparation for possible natural disasters and man-made accidents or incidents, such as fire, flood damage, riots, and more, Ping An has implemented corresponding physical environmental protection measures.