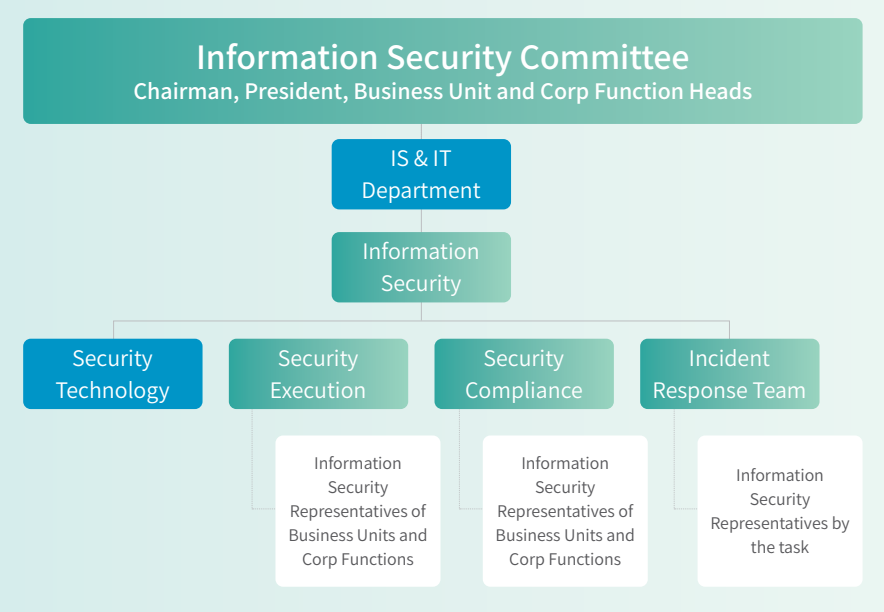
2.5 Information Security and Privacy Management

LITEON values the privacy and safety of its stakeholders, including employees in the company, outside partners (customers, suppliers, and consultants), and shareholders, and of operation related information assets. In 2018, LITEON worked hard to make the company's information security system comply with ISO 27001: 2013, and implemented the Information Security Policy to provide the basis for management. Meanwhile, in response to the requirements of the General Data Protection Regulation (GDPR), LITEON, for the purpose of ensuring the collection, processing or use of personal information complies with the GDPR, the Personal Information Protection Act of the Republic of China and related regulations, and the competent authorities' requirements, started amending the Personal Information Protection and Security Policy ("the Policy") and related guidelines in 2020. As a guide for personal information protection tasks, the Policy is implemented in all LITEON offices worldwide, and a cross-departmental and cross-functional information security organization is in place to perform information security related tasks. Meanwhile, information security management tools are being introduced on an ongoing basis, and information security mechanisms are constantly being strengthened in order to maintain effective and operational information security and privacy protection. No complaint relating to invasion of client privacy or loss of customer data was made in 2020.

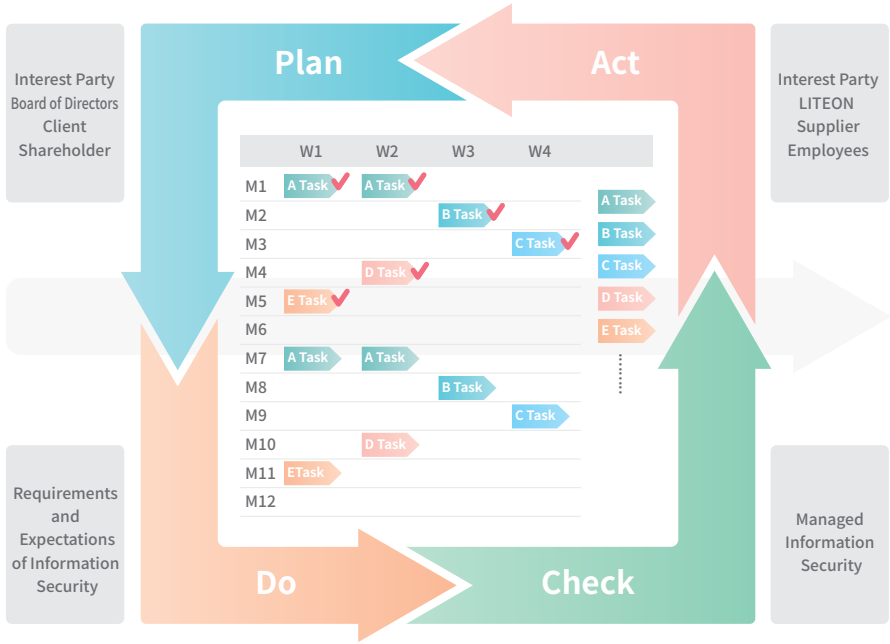
Information security organizational structure

In 2018, the cross-departmental and cross-functional Information Security Committee was created with the chairman and president serving as the convener. In 2020, the Information Security Department was renamed from InfoSec to be Information Security and combined into IT Department as the part of the IS & IT Department to be responsible for information security operations and emergency response and recovery. The IS & IT Department's mission is to prevent information security breach and reduce losses arising from such incidents.



Information security management and audit mechanisms

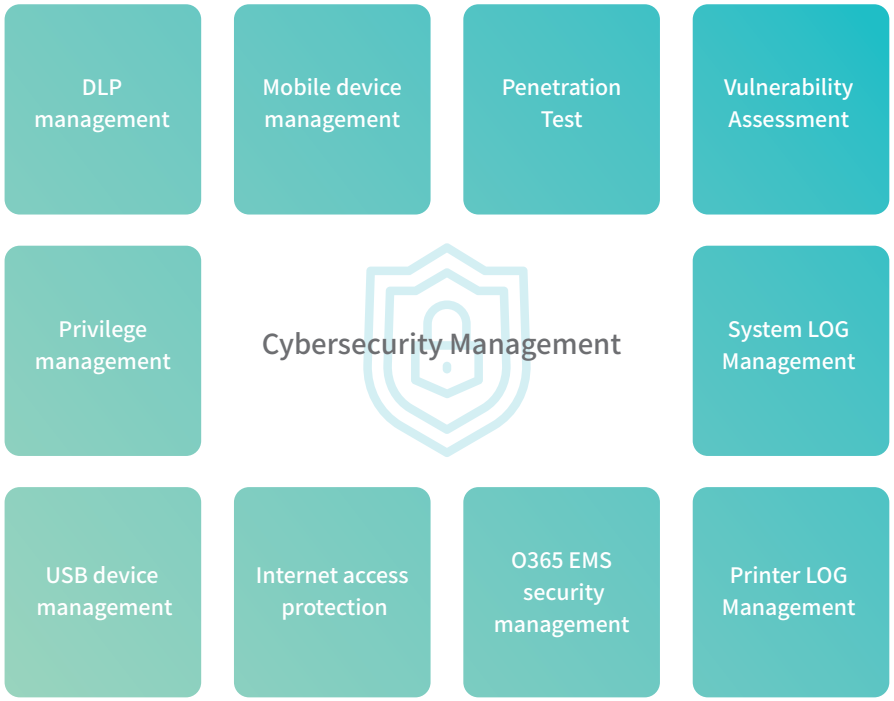
To ensure effective implementation of information security management mechanisms and maintain confidentiality, integrity, and availability of information assets, LITEON follows the ISO 27001: 2013 standards to implement information security management system documents, and uses the PDCA cycle to create, implement, maintain, and improve information security management systems. LITEON obtained ISO 27001 information security management system certification in 2020. Meanwhile, LITEON built and trained an information security audit team in 2020. All auditors on the team obtained ISO 27001: 2013 Lead Auditor certification.



Implementation of information security technology controls

1. An information security monitoring system has been implemented to perform system vulnerability scanning and prevent hacker attacks and theft of confidential information. The complete information security network includes server rooms, network equipment, network connection, and personal IT equipment (e.g., desktop and laptop computers, tablets, and smartphones). The network is intended to ensure personal information, confidential business data, and customer and supplier information are effectively protected.

2. The Azure Information Protection (AIP) service is introduced to ensure LITEON data are protected. The AIP service uses digital cloud tools, such as Microsoft Office 365 and encryption, identification, authorization rules, and secure remote access, to protect employee information and confidential business documents.



Information security education and training

To raise awareness of information security among employees, LITEON added the Personal Information Security Requirements and Training Administration Procedures to the information security management system documents to provide a basis for management.

1. Information security awareness campaigns: Information security news are announced, and campaigns conducted via various channels as needed to raise information security awareness in the workforce.

2. Information security education and training:
   (1) To provide a better understanding of its information security policy, LITEON requires new employees sign the employee code of conduct agreement and receive information security training on the same day when they join the company.
   (2) LITEON provides routine information security training for employees every year. All employees are required to complete a minimum of one hour of information security training every year. Information security courses on different topics are organized for employees based on their roles and responsibilities. A minimum of six information security and privacy courses were created this year. LITEON provides ongoing training as a means to raise information security awareness in the workplace and incorporate the elements into the processes in order to achieve the most secure and rigorous information protection.
   (3) In addition to training provided by LITEON, primary information security representatives and information security auditors are required to participate in training activities or seminars organized by outside parties. The requirement is intended to enhance information security for LITEON by sending the information security personnel to learn more about information security mechanisms and the latest forms of information security attacks.
   (4) Social engineering exercises are conducted as needed every year to raise information security awareness among employees.

Information security control mechanism	Description	Information security risk management
Privileged account management	Privileged local administrative account management system for clients	Prevent employees from installing illegal or pirated software or malware attacks
Peripheral management	Peripheral access and storage control system for clients	Prevent employees from leaking confidential/sensitive information via portable storage devices
Internet access control	Internet access control and threat detection system	Prevent employees from visiting malicious websites and incurring cyberthreats and virus attacks
Data leakage control	Data loss prevention (DLP) for computer data leakage prevention on client computers	Detect, record, and track confidential/sensitive information leakage
Data leakage control	Conditional access allows O365 access only on company computers	Prevent confidential/sensitive information leakage and hacker attacks
System vulnerability control	Desktop computer vulnerability scanning and detection system	Provide computer vulnerability check reports and prevent threats and attacks
Log audit control	Desktop computer log tracking and management system	Provide relevant information security audit event trace logs for inquiry
Network threat control	Unusual traffic volume and threat detection system for office and factory networks	Prevent the spread of online ransomware
Mobile device access control	MAM (Mobile APP Management)/ MDM (Mobile Device Management)/ MTD (Mobile Threat Detection) systems	Prevent employees from using personal mobile devices to leak confidential/sensitive information and cyberthreats
Remote access control	Remote access control for remote connections	Provide employees with an IT application system for accessing the company's systems remotely