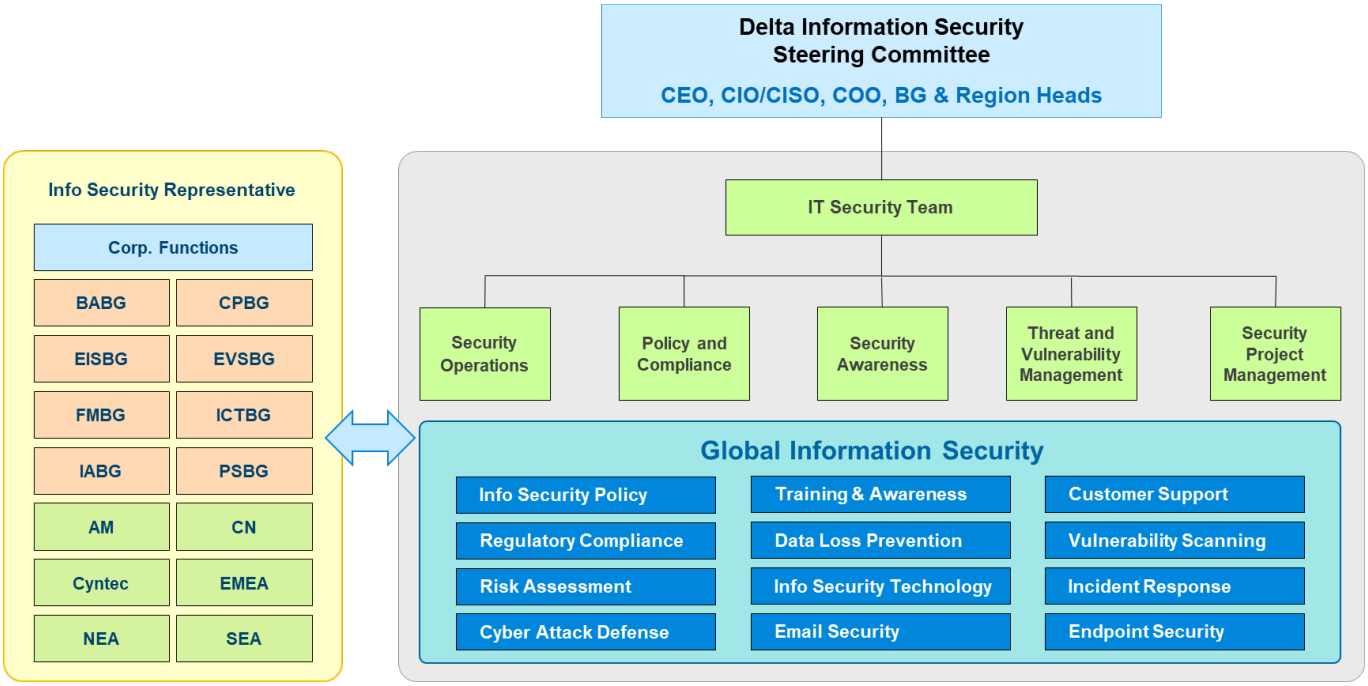
Implementation of Delta Information Security

▶ Cyber Security Management

1. Organizational Chart of Delta Information Security

The Company has set up an Information Security Steering Committee, chaired by the CEO and with its Chief Information Officer as the Chief Information Security Officer and senior executives from all global business groups and regions as Committee members. The Information Security Department has also been established to oversee Delta's information security and physical security planning and related audits, and to facilitate the operation of this Committee. Through quarterly management review meetings, the Information Security Steering Committee reviews the results of information security risk analysis and the corresponding protective measures and policies adopted by the Company to ensure the suitability, appropriateness and effectiveness of the ongoing operation of the information security management system. The Chief Information Security Officer reports annually to the Board of Directors on the effectiveness of information security management and the direction of the information security strategy to ensure that information security policies and controls are implemented in Delta's business units around the world. This year (2023), Delta Chief Information Security Officer reported overall Delta Information Security governance to the Board of Directors on April 27 and the Board of Directors also approved the amendment to Delta Group Information Security and Personal Information Protection Policy.



2. Delta Information Security Policy

The Company's information security policy covers the Company and its domestic and overseas subsidiaries and is based on the following guiding principles: "1. Maintain an appropriate level of information security to ensure the confidentiality, integrity, and availability of information assets; 2. Ensure the security of the Group's information and prevent the leakage or loss of important information; 3. Maintain consistency in the Group's operational environment and information security, while considering both information security and information sharing; 4. The Group's information security policies and procedures shall be established in compliance with applicable information security laws and regulations." The goal is to protect Group's information assets from unauthorized or accidental modification and destruction by building up threat prevention, detection, and response solutions, and establishing backup plans

and disaster recovery programs. The policy will be evaluated and reviewed annually in accordance with changes in government laws, environment, business and technology and any amendments of policy will be announced and conducted after approved by the board of directors. We also held the courses of information security policy for the Group's employees every year to enhance their information security awareness.

In order to effectively implement information security management, we hold monthly meetings with information security managers in overseas regions to review the applicability of information security policies and protection measures based on the management cycle of Plan-Do-Check-Act (PDCA), and report the effectiveness of implementation to the Information Security Committee on a regular basis.

In the "project phase", we focus on information security risk management. In order to strengthen information security, the Company has introduced ISO27001 information security management system certification since 2018, so that the information system can operate under standard management norms to reduce security loopholes and production abnormalities caused by human error and continue to improve through annual review operations.

In the "execution phase", we have established a multi-layered information security protection mechanism, continued to renew information security solutions, enhanced the efficiency of the detection and response procedures for various information security incidents through intelligent/automated mechanisms, and strengthened the information security and network security protection processes to safeguard the Company's critical assets.

In the "inspection phase", the effectiveness of information security management indicators is regularly monitored. The management system mentioned above undergoes an annual third-party review and audit. In addition, renowned cybersecurity companies are commissioned to conduct penetration testing to ensure our continuous improvement of information security management and defense capabilities.

In the "action phase", continuously improve people, process, technology to enhance security management efficiency.

3. Specific management solutions

In order to achieve the information security policy and objectives and to establish a comprehensive information security protection, the management issues and specific management plan are as follows:

- Enhance information security defense capability: We regularly conduct system information security vulnerability analysis and penetration tests every year, and patch and repair them to reduce information security risks. Establish a network security incident response plan, evaluate the impact and loss according to the severity level of the incident, take corresponding notification and recovery actions, and execute regular information security incident response drills.
- Enhance network, endpoint and application security: Implement SIEM (Security Information and Event Management) system to aggregate and filter security events and logs from network protection systems (e.g., firewalls, intrusion detection systems) and critical systems for automated connectivity analysis and monitoring to detect and identify network security threats and attacks, and to provide real-time alerts according to predefined rules. We also optimize the overall information system network security compartmentalization, and in addition to multi-factor authentication for remote login of colleagues, multi-factor authentication protection is also provided for privileged account login to important hosts.
- Regulatory compliance and introduction of international security certification standards: To enhance the information security management and personal data protection mechanisms of the Company, as well as to ensure compliance with relevant regulatory requirements, we expanded the scope of ISO 27001 information security standard certification to include the European region in the year 2022. In addition, we implemented the

ISO 27701 personal data management system to strengthen personal data management security and obtained the international certificates of ISO 27001 with the expanded scope and ISO 27701 through external third-party verification in October 2022. The certificates are valid from October 2022 until August 2024. The Company will continue to strengthen the security protection of its information infrastructure and application systems and adequately implement mechanisms for data security and personal data protection.

- Risk Management: The Company utilizes the systematic risk management methods provided by ISO 27001 and ISO 27701 to identify, assess, and manage information security and personal data protection risks faced by the organization. These standards emphasize comprehensive risk assessments of information assets and personal data, as well as the development of corresponding risk management measures based on the assessment results. Additionally, we collaborate with large international information security companies to conduct comprehensive information security inspections, using their professional services so as to enhance advanced information security based on the objective results from third-party verification. We are also a member of TWCERT and regularly collect cybersecurity threat intelligence to take appropriate preventive measures to reduce potential risks to the Company.
- To strengthen employees' awareness of information security: In addition to annual information security awareness training for Delta employees worldwide, we also conduct phishing email drills and phishing email recognition awareness training for employees, and analyze the results of the drills to continuously improve the effectiveness of the drills.
- Epidemic Control: In response to the global COVID-19 pandemic, we strengthened the antivirus and information security measures for Work From Home (WFH), discouraged the use of public computers and networks for work purposes, and fulfilled the responsibility of protecting company information.
- In response to digital transformation, more automated integration solutions are being promoted to enhance cybersecurity resilience, particularly focusing on cloud security.

4. Information security management resources invested

Information security has become an important issue in the company's operation, and the information security management issues and resources invested are as follows:

- Dedicated manpower: We have a dedicated 1 Chief Information Security Officer and 14 people in the "Information Security Department", which are responsible for our information security planning, information security system operation, technology introduction and related audits to maintain and continuously strengthen information security. The Company has also established local information security representatives in various regions worldwide, holding monthly meetings to discuss information security-related matters.
- Education and Training: All newly hired employees complete information security educational training courses before starting with the Company and are required to sign the information security policy statement. Each year, professional technical and managerial staff around the globe are also required to complete annual information security educational training and pass relevant assessments. In the year 2023, an annual information security training was delivered to all Group employees, including content on cybersecurity awareness, data protection, social engineering, and information security policies. The information security department also issues information security newsletters based on current events to inform employees about the latest information security risks, zero-day vulnerabilities, and more. Meanwhile, to enhance awareness of phishing emails among the staff members, the information security department conducts at least two social engineering phishing email drills for all global employees every

year.

5. The impact of historically severe information security incidents and countermeasures

Delta was attacked by hackers in January 2022, causing abnormal operation of the Company's official website, Office Automation for office works and relevant systems. After detecting the system abnormality, the IT department immediately notified the relevant internal units to activate the information security incident response mechanism and invited external information security experts to collaborate on the incident response to curb the spread of malware and attack methods. In addition, we also promptly located the affected systems and immediately recovered them. Therefore, this incident did not cause any significant impact or loss to the Company's overall operation. Meanwhile, the Company has reported the incident to the competent authorities and law enforcement agencies and published material information according to legal regulations.

The forensic analysis and investigation of the incident concluded that the hackers obtained the accounts of the Company's employees through social engineering, and then hacked the Company's computer system through the internet to launch the attack. In response to the increasing threat and risk of hacking attacks, Delta's information security unit has enhanced information security training and phishing email drills for Delta employees worldwide, optimized the suspicious email filtering mechanism, and continued to enhance the monitoring mechanism to detect network threats and strengthen security control measures for critical system services to reduce information security risks and prevent the recurrence of similar hacking attacks.