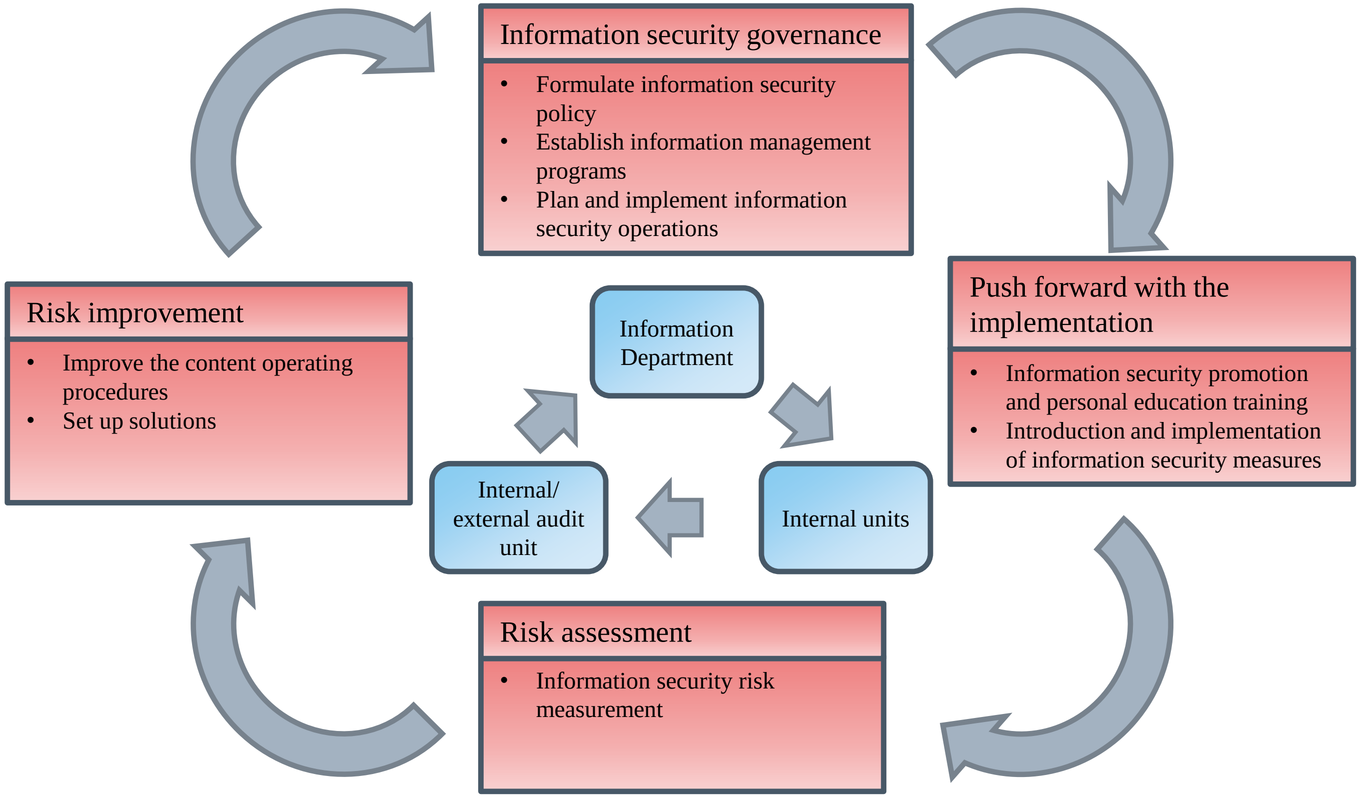
- Information security risk management framework, security policy and concrete management programs were reported to the Board of Directors on 28 June 2024
- Establish information security risk management framework



Information security governance

- Formulate information security policy
- Establish information management programs
- Plan and implement information security operations

Push forward with the implementation

- Information security promotion and personal education training
- Introduction and implementation of information security measures

Risk assessment

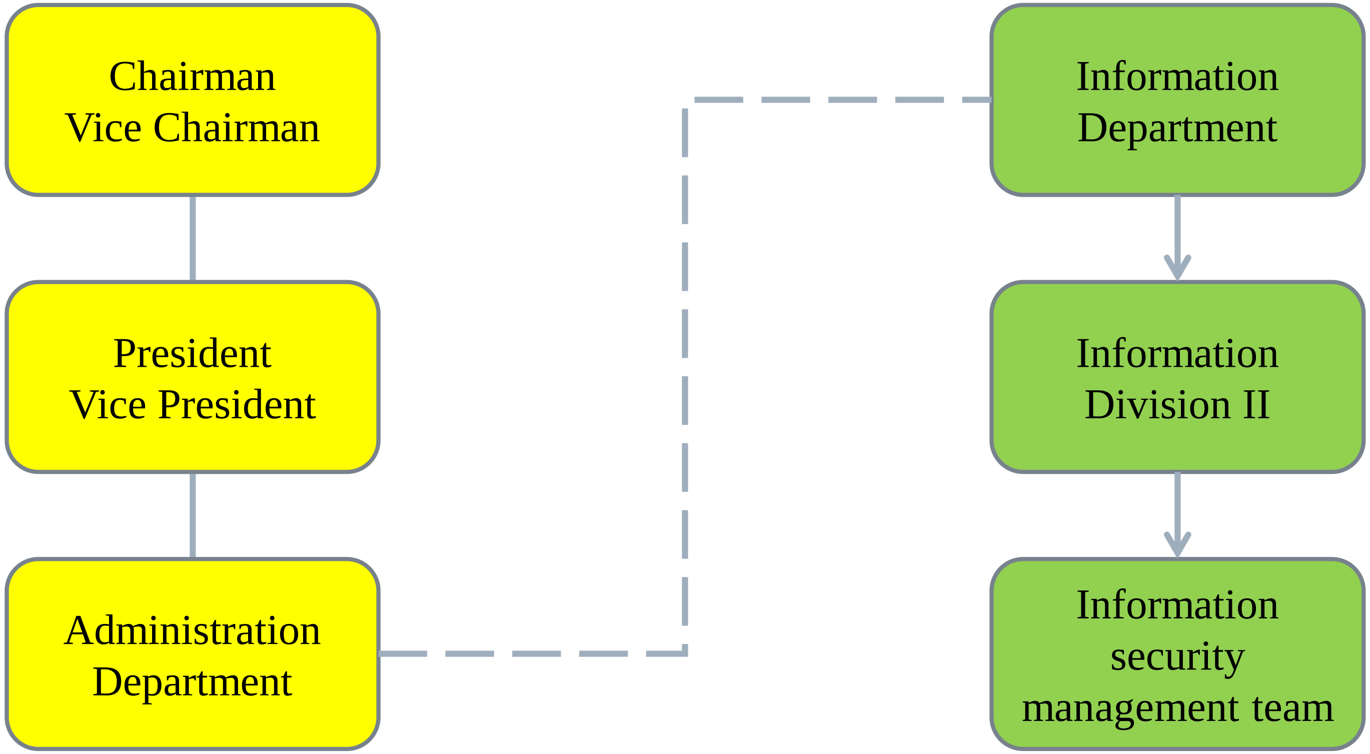
- Information security risk measurement

Risk improvement

- Improve the content operating procedures
- Set up solutions

Information security organization and structure

- Information security organization and structure (establish a designated unit in charge of information security and establish the position of Information Security Supervisor)



Remarks:
An Information Security Supervisor and Information Security Specialist were reported in an announcement according to the rules in April 2022.

Information security policy

- The purpose of Kenda Industrial Company’s information security policy: maintain overall information security, strengthen the security management of various information assets to ensure their confidentiality, completeness and availability to meet the needs of business operation.
  - Compliance with the laws and regulations of the government: comply with all relevant laws and regulations and information security regulations, and strive to maintain the security of all information to meet the stable operational needs of the enterprise.
  - Revision of information security management measures in a timely manner: through the process of internal and external security threat and risk assessment, the information security management measures are revised in a timely manner to eliminate risks.
  - Strengthen the employees' awareness of information security: conduct comprehensive information security education and training, strengthen all employees' capability and awareness of information security and create an environment for corporate information security.

Information security policy

- Maintain the confidentiality, availability and completeness of computer data: a complete data redundancy/backup mechanism to ensure that the computer data in the enterprise can be used effectively at any time.
- Grasp or introduce the latest information security products: maintain contact with information security vendors to obtain the latest knowledge on information security and protection, introduce new information security products when necessary, and keep the enterprise information security system in sync with external technology.

Concrete management programs of information security

- Information security management programs
  - Security management of information machine room
  - Password management
  - Information technology protection
  - Information file control
  - Information backup/redundancy and recovery
  - Information security management promotion
  - Handling of non-compliance
  - Conduct audits regularly

(Each program is described below)

Information security management programs

- Security management of information machine room
  - The information machine room is locked at all times and the access control card is managed by the network administrator and kept in safe custody.
  - The matters handled by the information personnel in the machine room are recorded in the relevant log book. If people outside the factory wish to enter the machine room due to business needs, they must be accompanied by the information personnel. At the same time, the name of the person entering the machine room, the time of entry and exit and a summary of work are recorded in the visitors' entry and exit records.
  - The temperature of the machine room is kept below 28 degree Celsius, and the humidity is kept between 30%~65%. The person on duty records the temperature and humidity of the machine room. There should be two sets of air-conditioning equipment which are interchangeable and have security and emergency lighting equipment inside. Checks are performed once a week.

Information security management programs

- Contingency response and educational training is held at least semi-annually to familiarize with the operation.
- Yuanlin Factory, Yunlin Factory and global research and development headquarter are equipped with information machine rooms, but Douliu Factory and Taipei office are not equipped with information machine rooms.

Information security management programs

- Password management
  - If a personal computer is left idle for more than 15 minutes, the screen saver will be automatically activated and locked. The personal computer is prohibited from writing files to external storage devices. If a MEMO has to be submitted due to business needs, the file can be written only after obtaining the approval of the supervisor at the level of assistant manager or above.
  - For colleagues who perform special business or have a highly confidential nature, the AD password length should be set to 7 codes and a combination of English letters and numbers. There will be an automatic reminder of the system at the expiration of the windows password after 90 days and expiration of UNIX ERP after 13 weeks.
  - Set up programming and data access requirements.

Information security management programs

- Information technology protection
  - As part of the Company's information security checks, network security procedures are established to prevent tampering or modification of business information.
  - Use a network firewall and a designated person will be in charge of it. The following functions will be enabled:

    1. Web filtering: filter malicious URL.
    2. Intrusion protection: filtering suspicious packets and network traffic for malicious attack packets.
    3. Botnet protection: detects malware by analyzing its network protocols.
    4. Virus protection: filtering viruses in network transmission.

Information security management programs

- Use mail protection: use spam mail host to prevent the attack of external mass mail traffic, and detect and analyze mail content to filter malicious virus.
- Personal computers are installed with anti-virus software and virus codes are updated regularly.
- Anti-virus software is fully used. Virus code is automatically updated by anti-virus server every hour and automatically deployed to each computer.
- On 4 May 2022, we joined the joint security organizations CERT/CSIRT in Taiwan to obtain the latest information security information on a regular basis.

Information security management programs

- Information file control
  - Rules on the management of sensitive and material information
  - Managed according to the confidentiality level defined by the "Standardized procedures and confidentiality principles within the Company".
  - Information of each department of the Company is stored in groups in network hard disk shared resource, and our network hard disk fileserver and kdfile hosts are shared in accordance with the "Regulations on information security inspection".

Information security management programs

- kdfile is for confidential files as mentioned in the second category below and fileserver is for non-confidential files as mentioned in the third category below. Classified by departments/units with access rights control and set to be read-only or writable depending on the nature of the file.
- Folders are divided into three main categories:

1. The first category is public read-only (e.g., announcements, SOP documents, rules and regulations).
2. The second category is departmental folder which can be read and written by colleagues in the same department, while other departmental/units do not have any permission.
3. The third category is departmental public folder which is primarily read and written by the same departmental/unit, while other departmental/units only have read-only access.

Information security management programs

- Information backup/redundancy and recovery
  - The backups are divided into UNIX server, E-MAIL server and Microsoft server in the machine room.
  - UNIX server: backup of database every night at regular intervals; backup of the modified programs and files of the previous day twice a day; backup of all data in the database every Sunday and store the tapes offsite; backup messages should be recorded on the computer tape records.

Information security management programs

- Microsoft server: mainly for Microsoft SQL database and related programs.
- Spot test of backup data recovery verification shall be conducted once every six months for each system to check the validity of the backup data, and the test status will be recorded in the server room records.
- Building of important server redundancy structure.

Information security management programs

- Information security management promotion
  - The supervisor of Information Department develops information security policy.
  - The supervisor of Information Network Management Department conducts annual training for employees and keep a record.
  - Rehearsal is held once a year.

Information security management programs

- Handling of non-compliance
  - Users of the Company's network are required to abide by the Company's network regulations. If any of the following incidents occur and are found to be true, the Company will restrict the use of the network and, in the event of a repeat offender or serious case, the Company will issue a request to the Human Resources Evaluation Committee for punishment according to the circumstances.
  - The information unit has proposed a clause in the outsourcing contract that requires the outsourced entity to comply with confidentiality requirements and assume legal obligations.

Information security management programs

- Conduct audits regularly
  - The Company conducts an audit of information system according to the annual audit plan of the Office of Internal Audit.

Quantitative Data on Resources Invested in Information Security Management

Resources for information security management

- Regular renew antivirus/firewall software and update
  - Actual Investment in 2023: Approximately 650,000
  - Actual Investment in 2024: Approximately 740,000 (an increase of 13.9% compared to last year)
- Signing of Maintenance Contracts for Important Information/Network Hardware
  - Actual Investment in 2023: 700,000
  - Actual Investment in 2024: 700,000 (investment remains the same)
- New Purchase of Firewall for R&D Department in 2024
  - Purchase of firewall for R&D department approximately 1.58 million

Quantitative Data on Resources Invested in Information Security Management

Resources for information security management

- Firewall Communication Policy / Cybersecurity Protection Improvements
  - Total Improvement Cases in 2023: 12 cases
  - Improvement Cases in 2024: 6 cases (1 more than last year)
- Implementation of "Information Security Training" for All Employees
  - Total Training Hours in 2023: 3958.5 hours
  - Training Hours in 2024: 162 hours (as of May 2024)
- Implementation of Computer Replacement and Upgrades
  - Total Actual Investment in 2023: Approximately 2.93 million
  - Actual Investment in 2024: Approximately 1.76 million (an increase of 63.8% compared to last year)

Future prospects

- Enhance management of information security risk
  - Information security system inventory: request the vendors to assist in carrying out the Company's information security risk assessment
  - Information security risk improvement: evaluate the purchasing of information security system equipment according to the risk assessment report
  - Information security vulnerability scan: carry out Company-wide information security vulnerability scan
- Assessment of obtaining information security management system standard certification through a third party
- Moderately introduce cybersecurity monitoring management equipment, asset management inventory software, upgrade server operating systems, and update firewall hardware.