the "Information Security Management Review Committee" and "Trade Secrets Committee"

Following the global development of Fintech, the information security risk to be dealt with by enterprises is increasing day by day. Meanwhile, in order to protect the staff's painstaking results, the Company established the "Information Security Management Review Committee" and "Trade Secrets Committee" in 2010 and 2018.

Information Security Management Review Committee

The Committee holds the meeting once per six months, which shall be attended by the Committee members. The meeting is held in April and October of each year and responsible for reviewing and resolving the (1) information security policy, (2) validity of the information security policy and control measures, (3) resources required by information security. The structure, information security policy and specific control programs of the Company's information security risk management are stated as following:

1. Policy and principles
   (1) The information risk assessment on information assets shall take into account the related laws and business needs, in order to ensure the needs for information security, establish the standard operating procedures, take appropriate information security control measures and ensure the security of information assets.
   (2) Establish the assessment or appraisal system based on the personnel's functions and competencies, and organize the information security educational training and promotional activities, if necessary.
   (3) The granting of the right to access information assets shall be subject to the business needs and take into account the minimum authority, separation of responsibilities and review of independence.
   (4) Establish the information security incidents management procedure to ensure timely response to and control and processing of any incidents, and prepare the business continuity plan and perform periodic drills to ensure the continuing operation of the information system or information service.
   (5) Process and protect personal information and intellectual property rights in accordance with the Personal Information Protection Act and intellectual property rights.
   (6) Conduct the information security audit periodically to ensure that the information security management system is practiced.
   (7) Any violations of the policy and information security-related requirements shall be subject to the punishment rendered by related laws or the Company's personnel regulations.
   (8) Establish the "Declaration of Information Security" for the Company's staff separately, in order to ensure that the staffs are aware of the Company's information security requirements.

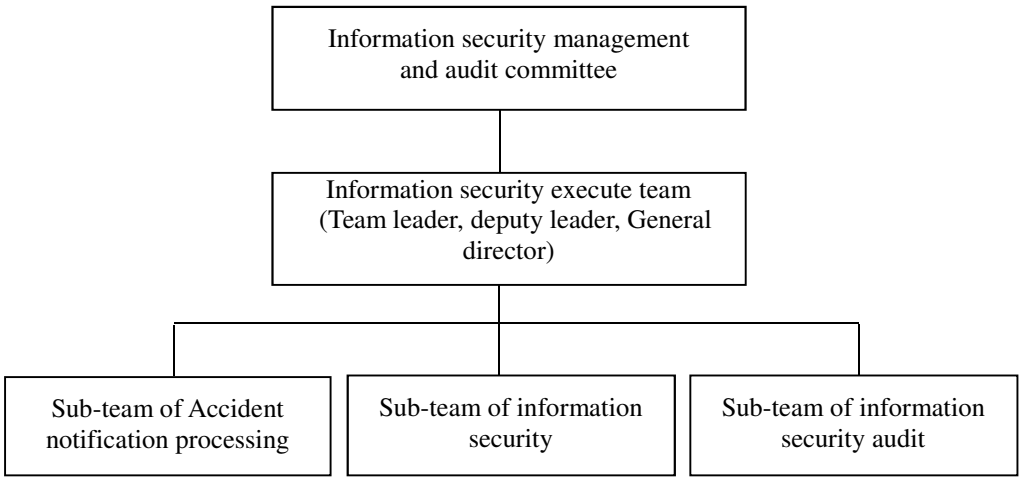
Declaration of Information Security

The ultimate goal for the Company's information security operations resides in: ensuring the effective operation of the Company's key business information processing operations through the control over personnel, operations and information technology to prevent any security incidents about confidentiality, completeness and availability affecting the key business operations from arising during the processing of information and support the Company to achieve the goal for becoming a global photoelectrics manufacturing center.

The Company's information security operations are based on the systematic risk assessment and risk management, and implement the risk control measures by weighing management and technology evenly. The same are practiced by the staff in their daily life, so that they may work with each other to realize the Company's information security goals identified as following:

- The protection of information related to key business completely satisfies the Company's requirement and related laws & regulations.
- The information processing procedure and processing result for key business and support of administrative operations shall be accurate and correct completely.
- The information system and information processing services shall be non-interrupted.

2. Structure



3. Members, operations and functions

(1) Committee members

President, VP of Information Technology Center, internal auditor officer, Director-General of Intellectual Property & Legal Affairs Div., and manager of Legal Affairs Dept. of Intellectual Property & Legal Affairs Div.

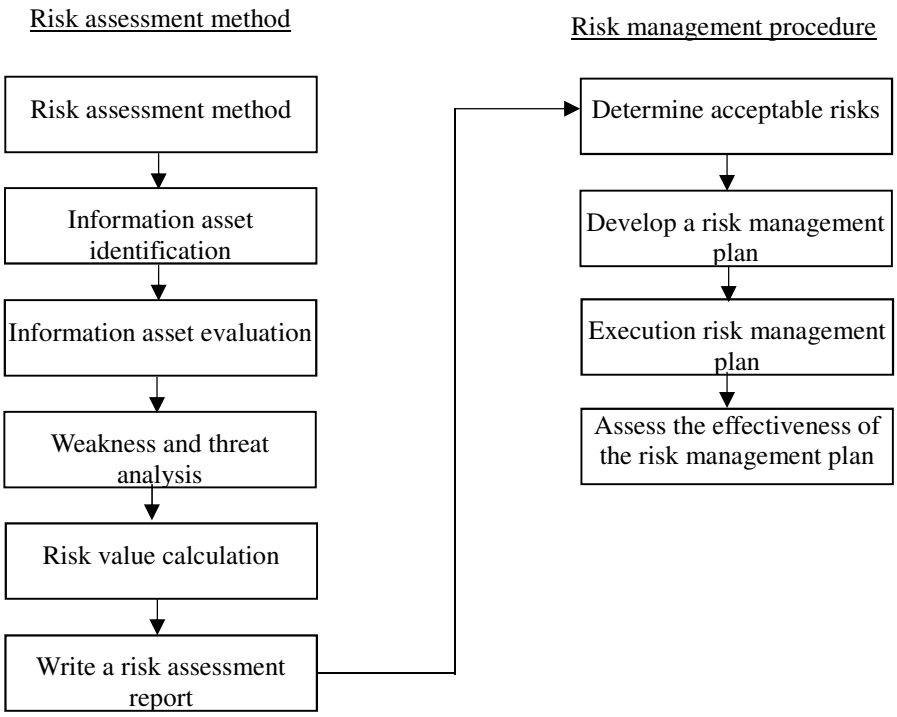
(2) Execution team members

Team leader, deputy leader and secretary

(3) Operations & functions

Position/Role	Operations & Functions
Information Security Management Review Committee Chairperson	● Responsible for reviewing and resolving the motions related to the Company's information security management. ● Review and approve information security policy. ● Review the validity of information security policy-based goals and control measures. ● Review the scope of resources required by information security.
Information Security Management Review Committee Convener	● Responsible for reviewing and resolving the motions related to the Company's information security management. ● Review and approve information security policy. ● Review the validity of information security policy-based goals and control measures. ● Review the scope of resources required by information security. ● Coordinate information security-related operations. ● Continue to improve information security management system.
Information Security Management Review Committee Member	● Responsible for reviewing and resolving the motions related to the Company's information security management. ● Review and approve information security policy. ● Review the validity of information security policy-based goals and control measures. ● Review the scope of resources required by information security.
Information Security Execution Team Leader	● Select competent personnel based on the specific information security role and position. ● Maintain the awareness toward information security. ● Coordinate information security-related operations. ● Confirm information security risk and implement risk management. ● Conduct independent audit on information security management system. ● Continue to improve information security management system.
Information Security Execution Team Deputy Leader	● Help the team leader select competent personnel based on the specific information security role and position. ● Help the team leader maintain the awareness toward information security. ● Help the team leader coordinate information security-related operations. ● Help the team leader confirm information security risk and implement risk management. ● Help the team leader conduct independent audit on information security management system. ● Help the team leader continue to improve information security management system.

4. Risk evaluation procedure and risk management procedure



5. Timing and approach to conduct the risk evaluation

(1) Timing to conduct the risk evaluation

- The risk evaluation shall be conducted once per six months, and the scope of evaluation shall be decided by the Information Security Execution Team Leader.
- In the event of changes in organization, operating procedures or information assets, or outbreak of material information security incidents, it is allowed to conduct the risk evaluation on information assets falling in the specific scope.

(2) Approach to conduct the risk evaluation

- The value of risk (RoA) of information assets consists of such elements as the value of information assets, vulnerability of assets, possibility of threats and effect thereof, and is calculated by multiplying by the value of information assets, vulnerability and possibility of threats and taking into account the effect produced by the threats on the confidentiality, completeness and availability.
- Identification of information assets (identification and inventory taking) refers to the inventory taking of information assets pursuant to the “Operating Procedures for Managing Information Assets” (PIS090003).
- Valuation of information assets (assessment on value) refers to the evaluation conducted by the information assets owner on the confidentiality, completeness and availability, and subject to the characteristics of organization, and requirements by laws and regulations.

6. Management system/internal audit/periodic reporting to Board of Directors / preventive measures

(1) Frequency of audit

Conduct the information security internal audit per six months (may be integrated into the Company's internal audit operations, if necessary), and conduct the audit on such specific purposes as information security incidents and material changes in the information system from time to time.

(2) Requirements about internal auditors

In order to ensure the objectivity and independence in the process of audit, the self-audit shall be avoided. The internal auditors shall have the experience in audit on information security systems or attending information security audit-related training programs (including the Company's internal training courses).

(3) Audit plan

- It is necessary to plan and prepare the information security audit plan in advance as the guide for audit. The contents thereof shall include the basis, scope, procedure, personnel, items and schedule of the audit, and executed upon approval of the Convener of Information Security Management Review Committee. The audit plan format may refer to the document numbers and standards under the information security management system.
- If the information security audit is integrated into the Company's interal audit operations, the information security plan shall be subject to the approval of the Convener of Information Security Management Review Committee and provided to the Audit Office to be included into the Company's internal audit plan for implementation.

(4) Reporting to Board of Directors

The contents about computerized information system processing and information security inspection have been reported to the Board of Directors on November 12, 2018, and relevant suggestions were posed toward the deficiencies. The deficiencies were followed up and corrected.

(5) Preventive measures

The Company has not yet taken out any information security insurance. Notwithstanding, the Company still spares no efforts to govern the information security and enhance its defensive ability. So far, no infringement upon suppliers' or customers' privacy, disclosure of confidential information or hacking into systems had been found.

The Information Security Execution Team performs the business continuity drill and information security phishing mail drill from time to time, and the restoration procedure in the event of any abnormality in the drilled system, and conducts period audits thereon. The

staff accepting the phishing mail shall attend the training and post-test about the information security phising mails again, in order to reduce the staff's chances to suffer attacks of virus, abducted encryption of data, disclosure of confidential information due to horizontal infection, or system invasion and paralisis.

Trade Secrets Committee

The information security is very important. Notwithstanding, it is also necessary to protect the security of the Company's trade secrets and a third party's confidential information held by the Company to ensure the staff's results, maintain the Company's competitiveness and prevent the Company's important information from being disclosed. On January 26, 2018, the Company formed the "Trade Secrets Committee".

1. Structure

   Formed by the President and the senior management of such units as Information Technology Center, Audit Office, Human Resources Center, Intellectual Property & Legal Affairs Div., and holding the meeting once a month.

2. Scope and duty of protection

   The confidential information includes any information, document, file, formula, product and sample of the Company and its subsidiaries which has not yet been disclosed to the public, or is identified confidential, sensitive or essential. Any violations of the regulations governing protection of trade secrets shall be punished upon the resolution made by Trade Secrets Committee, subject to the materiality of the case.

3. Implementation of educational training

   3.1. Periodic circulation of e-news to perform the educational training and promote laws & regulations to the whole staff.

   3.2. Irregular arrangement for related experts/trainees to perform educational training on specific employees