Taiwan Corporate Conduct and Ethics Implementation

Assessment Item	Implementation Status
1. Establishment of Corporate Conduct and Ethics Policy and Implementation Measures	
(1) Does the Company have bylaws and publicly available documents addressing its corporate conduct and ethics policy and measures, and the commitment regarding implementation of such policy from the Board of Directors and the management team?	Based on the policy being a prudent administrator; the Board of Directors and management are engaged in good management, loyalty, and honesty to implement the business. We've set Ethical Corporate Management Best Practice Principles. Please refer to Market Observation Post System or the Epistar's official website.
(2) Does the Company establish relevant policies that are duly enforced to prevent unethical conduct and provide implementation procedures, guidelines, consequence of violation and complaint procedures in such policies?	The Company strictly prohibits corruption, bribe and blackmail, establishes effective accounting system and internal control system, includes such promotional documents as employee handbook and employee reward & punishment regulations into the relevant anti-corruption guidelines and punishment against rule breakers, and provides employees with related educational training to ensure that each of the employees understand the related agreement and rules. The internal auditors will audit the status of compliance with said system. The Company also establishes the ethical corporate management best-practice principles, ethical code, operating procedure for prevention of insider trading and employees' complaining channels. For the relevant complaining mechanism, channel, and procedure please visit the Company's official website.

Assessment Item	Implementation Status
(3) Does the Company establish appropriate compliance measures for the business activities prescribed in Paragraph 2, Article 7 of the Ethical Corporate Management Best Practice Principles for TWSE/TPEx Listed Companies and any other such activities associated with high risk of unethical conduct?	The company abides by the laws and regulations in running business. Before the official information is announced, anyone involved is required to sign confidentiality agreement and shall not disclose important internal information to others. We also have strict control and precaution system about information security (IT).
2. Ethic Management Practice	
(1) Does the Company assess the ethics records of whom it has business relationship with and include business conduct and ethics related clauses in the business contracts?	The Company engages in commercial activities in a fair and transparent manner. Meanwhile, before engaging in any commercial activity, the Company will assess the trading counterpart carefully to avoid engaging in transactions with an unethical counterpart. When concluding the business contract with the trading counterpart, the counterpart needs to sign the letter of undertaking of integrity committing to bear legal liability and damages to maintain both parties' interest and right.
(2) Does the Company set up a unit, which is dedicated to or tasked with promoting the Company's ethical standards, and reports directly to the Board of Directors with periodical updates on relevant matters?	In order to well found the ethical management, the Company has Human Resources Center responsible for planning and executing various functions and reporting the result and seeking the budget approved by the Board of Directors on December 13, 2018, in addition to implementation of the project objectives. The president also assigns related units to help establish the ethical management policy and prevention program from time to time. To this end, the Company established the "Trade Secrets Committee" (see Page 140~143 for details) on January 26, 2018. The Company will organize the meeting each month, in addition to implementing the educational training. The Company releases e-news periodically and arranges the educational training offered by related experts for employees from time to time, and also disclose the status thereof in the CSR report and on the Company's official website.

Assessment Item	Implementation Status
(3) Does the Company establishe policies to prevent conflict of interests, provide appropriate communication and complaint channels and implement such policies properly?	We've established effective accounting and internal control system and operated smoothly. Complaints or reporting system also runs well so as to prevent corruption.
(4) To implement relevant policies on ethical conducts, does the company establish effective accounting and internal control systems that are audited by internal auditors or CPA periodically?	The Company has established an effective accounting and internal control system and operated smoothly. Internal audit members conduct regular audit as the planned schedule and make audit reports. Audit reports are sent for directors and independent directors for inspection so as to prevent corruption.
(5) Does the Company provide internal and external ethical conduct training programs on a regular basis?	Epistar will have a complete plan for employee development, we have a training roadmap according to each functional skill and position, and the employees can study through eLearning or participate in the internal training courses or register for external training courses through the training system. All employees could check detailed training records by themselves in the system. For the details about educational training on ethical management, please see as follow:

<table>
<tr><th>Assessment Item</th><th>Implementation Status</th></tr>
<tr><td></td><td>
Unit: NT$ thousand
<table>
<tr><th>Items of 2018</th><th>Attendee count</th><th>Hours of advanced studies</th><th>Cost of advanced studies</th></tr>
<tr><td>Series of management talents</td><td>218</td><td>1,159</td><td rowspan="10">5,664</td></tr>
<tr><td>Series of quality</td><td>1,100</td><td>3,979</td></tr>
<tr><td>Series of professionalism</td><td>2,429</td><td>5,988</td></tr>
<tr><td>Series of environment/safety/health (ESH)</td><td>6,573</td><td>53,692</td></tr>
<tr><td>Various series of professionalism</td><td>2,910</td><td>11,172</td></tr>
<tr><td>Orientation (including compliance with ethical management-related laws & regulations)</td><td>354</td><td>3,638</td></tr>
<tr><td>Compliance with laws and regulations on intellectual property right, protection of trade secrets and ethical manaement</td><td>203</td><td>50</td></tr>
<tr><td>Information security policy</td><td>216</td><td>54</td></tr>
<tr><td>Information confidentiality classification</td><td>3,526</td><td>882</td></tr>
<tr><td>Total</td><td>17,529</td><td>80,614</td></tr>
</table>
Said courses are primarily intended to conduct the educational propagation to the staff. The staff shall perform their duties with due diligence as a good administrator to protect the Company’s interest and right from being injured and satisfy the various stakeholders’ expection. During the orientation training for new employees, the Company strenghthens the propagation, and the new employees may review the online courses at any time in the “Crystal Collections” section on the Company’s intranet.
</td></tr>
</table>

Assessment Item	Implementation Status
3. Implementation of Complaint Procedures (1) Does the Company establish specific complaint and reward procedures, set up conveniently accessible complaint channels, and designate responsible individuals to handle the complaint received?	The Company sets up the independent email box and hotline available to complainants at the Company's internal portal website and official website. Any person who suspects or finds any violation of laws or ethical code may report the case to any of the following units and also provide sufficient information. If necessary, the Company will form a dedicated committee in confidential manner. The process of investigation and information related to the committee members, concerned parties shall be kept confidential, and the complainants' safety must be secured. The process shall also be reported to the Chairman of Board. 1. Immediate supervisor 2. Audit dept. supervisor, Human Resources Center/Employee Relations department supervisor or legal office & intellectual property right supervisor 3. The opinion response mechanism set up by the Company internally 4. The channel available to stakeholders 5. or other eligible personnel The opinion response mechanism not only offers the employees' complaining hotline but also sets up the opinion mailbox exclusive for employees. Employee Relations department acts as the dedicated unit responsible for organizing seminars for employees periodically, setting up the "being harassed while performing duties " hotline and mailbox, and organizing the "Heart Communication Meeting" chaired by President from time to time. Additionally, the complaint may be filed with Audit Department. Investor relations mailbox, CSR mailbox, customer service mailbox or channel available to stakeholders may serve as the external communication channel. The Company establishes ESH communication and consultation management procedure to enable the ESH management system to reach the consensus within the Company, and also establishes the ESH consultation and communication channel

Assessment Item	Implementation Status
	to the Company's external stakeholders. Any complaint will be processed as a special case promptly, and the process thereof will be reported to the Chairman of Board. Given this, the Company's complaining channels are considered perfect.
(2) Does the Company establish standard operation procedures for investigating the complaints received and ensuring such complaints are handled in a confidential manner?	Employee complaints and reports for offense are investigated in accordance with the relevant internal control procedures and the investigation committee is responsible for conducting investigations on relevant matters in a confidential manner and strictly protecting the reporters; unless otherwise provided by laws, the personal data and reporting materials provided by the reporters shall be kept confidential and we'll provide appropriate protective measures in accordance with the law to confirm that it has been dealt with by relevant protection mechanisms.
(3) Does the Company adopt proper measures to prevent a complainant from retaliation for his/her filing a complaint?	Strictly keep the complainant's identity, the process of investigation and related information confidential; if necessary, form a dedicated committee to conduct the related investigation. The members of investigation committee and relevant persons involved are required to keep confidential of the investigation process and related materials, and do their utmost to protect the safety of the reporters, and report the situation to the Chairman.
4. Information Disclosure Does the Company disclose its guidelines on business ethics as well as information about implementation of such guidelines on its website and Market Observation Post System ("MOPS")?	The Company discloses the information related to the Company in the investor service section and stakeholder section on the Company's official website at: http://www.epistar.com

Assessment Item	Implementation Status
5. If the Company has established corporate governance policies based on "the Ethical Corporate Management Best-Practice Principles for TWSE/TPEx Listed Companies", please describe any discrepancy between the policies and their implementation: None.	
6. Other important information to facilitate better understanding of the Company's corporate conduct and ethics compliance practices (e.g., review the company's corporate conduct and ethics policy): 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.	

Assessment Item	Implementation Status

(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

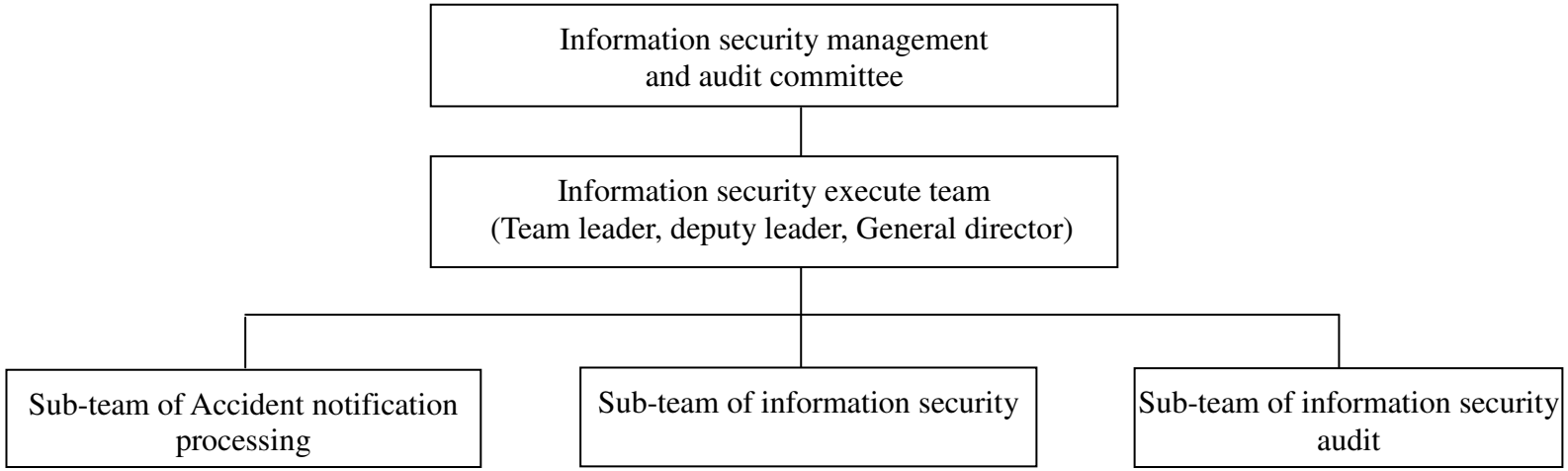
The ultimate goal for the Company's information security operations resides in: ensuring the effective operation of the Company's key business information processing operations through the control over personnel, operations and information technology to prevent any security incidents about confidentiality, 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.

Assessment Item	Implementation Status

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

Assessment Item	Implementation Status

(3) Operations & functions

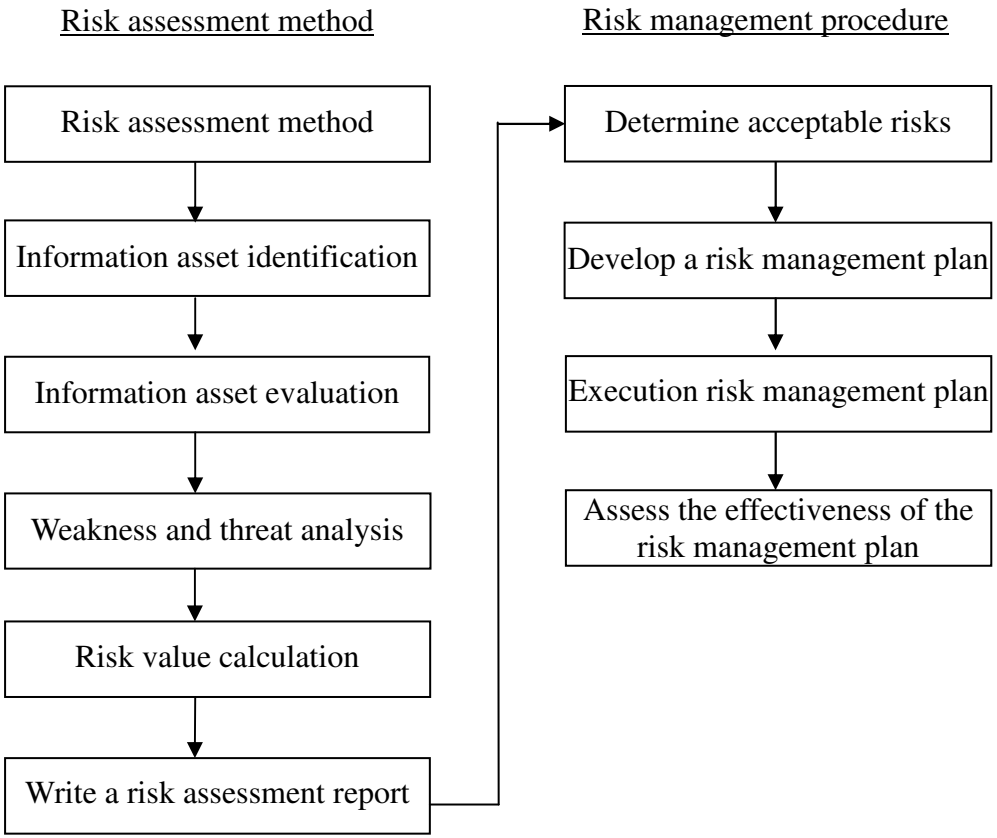
Position/Role	Operations & Functions
Information Security Management Review Committee Chairperson	● Responsible for reviewing and resolving the motions related to the Company's information security management. ● Review and approve information security policy. ● Review the validity of information security 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.

Assessment Item	Implementation Status

Position/Role	Operations & Functions
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.

Assessment Item	Implementation Status

4. Risk evaluation procedure and risk management procedure



Assessment Item	Implementation Status

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).

Assessment Item	Implementation Status
(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.	

Assessment Item	Implementation Status
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	