INTEGRITY AND ACCOUNTABILITY

3

ASEH commits to constructing sound corporate governance, conducting business ethically and complying with all laws and applicable regulations where we operate.

ASEH strives to establish an organizational culture of integrity and accountability, maintain high standards of ethics, effective corporate governance and accountability mechanisms in every aspect of its business, as well as conduct business based on the principle of social responsibility and business ethics to serve both the company's and shareholders' long-term interests.

2025 Key Performance

Continuous education for the Board members: 72 hours[1]

Continued listing on the TWSE Corporate Governance 100 Index (TWSE CG100 Index)

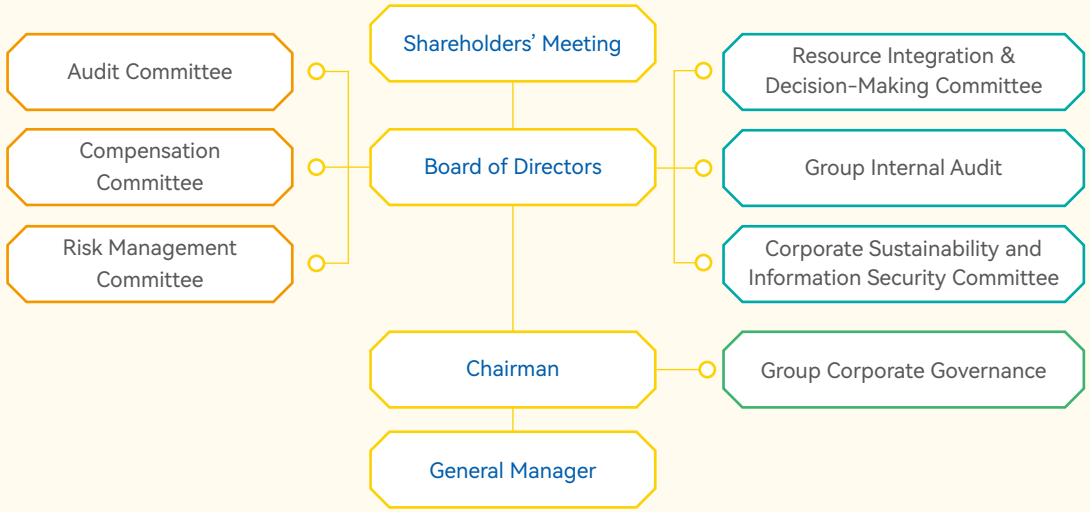
Performance Assessment of the Board and the Functional Committees

The company proactively reviews its corporate governance practices and effectiveness in implementation using the Corporate Governance Evaluation System launched by the FSC. A self-assessment process increases top management executives' awareness in strengthening corporate governance policies, and will help raise the standards of the company's corporate governance. In 2025, the company was among the top 20% best performing listed companies with better ratings in the categories of "Enhancing Board Composition and Operation" and "Promoting Sustainable Development". In 2025, the company was again selected to be a constituent stock of the "TWSE Corporate Governance 100 Index (TWSE CG100 Index)" based on the 2024 assessment of our corporate governance, liquidity tests and financial indicators. To achieve good corporate governance, we will continue to focus on increasing information transparency, protecting the rights and ensuring fair treatment of shareholders, and incorporating sustainable practices into corporate governance.

[1] Total training hours = course duration x number of people

3.1 Board of Directors

The board of directors of the company (the "Board") has established the "Audit Committee", "Compensation Committee", "Risk Management Committee" and "Corporate Sustainability and Information Security Committee"[1], which convene meetings in accordance with the charters approved by the Board, and perform duties conferred by applicable laws and regulations or by the Board. The functional committees shall submit proposals to the Board for resolution, and report to the Board on matters related to their functions and powers. In parallel, the Group Internal Audit Department conducts periodical audits and presents audit results to the Audit Committee and the Board. The Chief Administration Officer (Du-Tsuen Uang) was appointed as the Corporate Governance Officer to facilitate the operation of the Board[2]. In addition, the Resource Integration and Decision-Making Committee was established to strengthen resource integration and decision-making efficiency across all subsidiaries, with the goal of maximizing shareholder and stakeholder value.



[1] For further details on the composition and functions of the Audit Committee, Compensation Committee, Risk Management Committee, and Corporate Sustainability and Information Security Committee, please refer to our 2025 Annual Report (https://media-aseholdco.todayir.com/20260603162439498510721_en.pdf) and Form 20-F "Item 6 Directors, Senior Management and Employees – Directors and Senior Management" at https://media-aseholdco.todayir.com/20260407163248663671910_en.pdf or the company's website at https://ir.aseglobal.com/html/ir_committees.php

[2] For more details on the corporate governance affairs and training status of the Corporate Governance Officer, please refer to the company's website at https://ir.aseglobal.com/html/ir_corpor.php

[3] For further details on succession planning, please refer to the company's website at https://www.aseglobal.com/csr/integrity-and-accountability/succession-planning/

[4] Independent directors are as defined in Rule 10A-3 under the U.S.A. Securities Exchange Act of 1934 as well as defined by the Regulations Governing Appointment of Independent Directors and Compliance Matters for Public Companies by Taiwan FSC. The re-election of the company's directors was completed at the Annual Shareholders' Meeting in June 2024. A new director was elected to fill a vacancy by the 2025 Annual Shareholders' Meeting

[5] For further details on directors' attendance of meetings and information regarding conflict of interest, please refer to our 2025 Annual Report https://media-aseholdco.todayir.com/20260603162439498510721_en.pdf

Structure and Responsibilities of the Board of Directors

The Board is the highest governing body of the company. Jason Chang is the Chairman of Advanced Semiconductor Engineering Inc. ("ASE") since the company's listing on the Taiwan Stock Exchange in 1989. He is also the Chairman of the company since its founding in April 2018 and the Chair of the Resource Integration and Decision-Making Committee since 2021. As a strategic leader, the Chairman has led the company through consolidating core businesses, tackling challenges, and creating new business opportunities, to achieve market leadership in the semiconductor assembly and test industry. ASEH has developed a management succession plan and regularly evaluates the succession planning progress to ensure the company's sustainability[3].

The fourth Board consists of nine members, each serving a three-year term. Three of the members are independent directors[4]. In addition to the scope of authorities and duties granted by or in accordance with the Taiwan's Company Act, the company's Articles of Incorporation and Shareholders' Resolutions, the Board is actively engaged in the supervision of the overall operations of the company, business strategy formulation and development, risk identification in operation, finance, taxation, and overseeing, planning and implementation of ASEH's corporate sustainability. To strengthen independent oversight, the Company established the position of lead independent director and appointed independent director Mei-Yueh Ho as the first lead independent director by a resolution of the Board. In this role, she is responsible for hosting independent director meetings, aligning independent oversight perspectives, and facilitating effective communication between the independent directors and executive management.

In 2025, a total of eleven Board meetings were convened. Three independent directors attended every Board meeting in person to fulfill their supervisory duties. The average Board meeting attendance rate was 95.74%. To manage and avoid conflicts of interest, directors or the corporates they represent involving conflicts of interest which may jeopardize the interest of the company, are not allowed to participate in the discussions, exercise their votes, nor vote on behalf of other directors[5].

Diversity of the Board of Directors

The company's Corporate Governance Best Practice Principles lists the guidelines, management objectives and goals for selecting the Board members[1] and takes into account diverse and complementary factors such as: gender, age, nationality, culture, professional background and industry experience[2]. Members of the Board come from different professional backgrounds with global market perspectives and possess the abilities to conduct risk oversight.

Continuous Education for Board Members

To expand the knowledge and competencies of our Board members to effectively respond to evolving global and domestic corporate governance and sustainability challenges, a robust board education program was put in place. Based on industry requirements, educational and experience background of the Board members as well as the results from the performance evaluation of the Board, we facilitate the Board members with the course planning and activities. In alignment with prevailing global trends as well as internal risk assessments, the company organized training for the Board on topics including the strategic analysis of Taiwan–U.S. economic and trade relations and regulatory compliance in 2025. The Board members are also encouraged to attend external professional courses in accordance with their development needs. For example, some Board members have attended workshops in sustainable development performance and executive compensation, enterprise risk, and business continuity management. Our Board members have continued to participate in continuous education on corporate governance and sustainability during their tenure, with each director fulfilling the required annual training hours in accordance with applicable regulations[3].

Board Participation in Sustainability Governance

The Board has direct oversight and management of the company's ESG performance, and the authority to make decisions. In 2025, the Board passed the following resolutions – a) donating NT$100 million to environmental causes in Taiwan[4], and b) approved amendments to multiple policy documents pertaining to articles of incorporation, corporate value enhancement plan, sustainable development, corporate governance, risk management, guidance on prevention of corruption, business conduct and ethics, supplier management, environmental responsibility, biodiversity protection and no deforestation, and human rights. The Chief Sustainability Officer and Corporate Governance Officer is responsible for consolidating and reporting to the Board on company-wide implementation covering - GHG inventory, sustainable development, stakeholder engagement, regulatory compliance, ethics, risk management, information security management, intellectual property management, and IFRS Sustainability Disclosure Standards. In July 2025, to strengthen information security management, the Board resolved to elevate the status of the company's "Information Security Task Force" to a functional committee, and to rename the "Corporate Sustainability Committee" as the "Corporate Sustainability and Information Security Committee." The Board also approved the organizational charter of the Corporate Sustainability and Information Security Committee. The entire committee is composed of Board members and is chaired by the Chairman of the Board. This structure is intended to enhance the Board's oversight of the company's ESG performance and information security matters, including the annual implementation results, associated risks and opportunities, and future strategic planning.

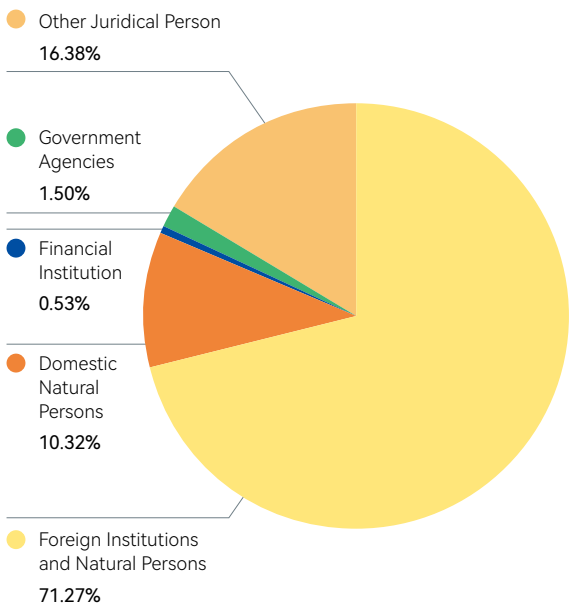
Board Performance and Remuneration

We have formulated remuneration policies for our Board member and top management to support strategy of sustainable business. The Compensation Committee evaluate the remuneration of directors and management on a regular basis according to the corporate governance trend report and the overall remuneration market competitiveness report. In addition to individual performance of current year, the remuneration of top management is also determined based on the achievement of the company's financial and relative financial[5] performance targets. The company has engaged third-party consultants to provide professional expertise backed by data from global research to help the Compensation Committee formulate and manage the Company's remuneration structure.

In 2021 and 2024, the shareholders' meeting respectively resolved to issue restricted stock awards as part of the top management's variable compensation package based on the integration of ESG metrics in greenhouse gas emission and water withdrawal intensity with the company's financial performance (consolidated operating revenue, consolidated gross profit and gross profit margin, consolidated operating profit and operating profit margin). Adopting an incentive plan that links ESG to financial results demonstrates ASEH's commitment to sustainable actions and results, while pursuing strategic business goals.

[1] For further details on the status of directors' diversity and management objectives and goals achieved, please refer to the company's website at https://cms.ase.todayir.com.tw/html/client_tw/ase/attachment/20260825155236210011884_en.pdf
[2] For further details on the composition of the Board, and professional backgrounds and industry experiences of Board members, please refer to 2025 Annual Report "Ch. 2. Corporate Governance Report" or 2025 Form 20-F "Item 6. Directors Senior Management and Employees — Directors and Senior Management"
[3] For more detail on continuous education for Board members, please refer to 2025 Annual Report "Ch. 2.3 Corporate Governance"
[4] Since 2014, ASE has donated NT$100 million annually and the program continue after the establishment of the company
[5] Relative financial performance targets such as revenue growth rate, etc

Structure of Shareholders



To enhance overall efficiency of the Board and to measure the performance of the Board on a yearly basis, individual members, and the functional committees with respect to leading and supervising the company's performance, we established a board of directors evaluation system that incorporates non-financial indicators as well as sustainability-related elements. In accordance with the Rules of Performance Evaluation of the Board of Directors, we have completed internal performance evaluations for the Board as a whole, and for individual directors and functional committees in 2025. Every three years, we commissioned an external professional independent institution to evaluate the Board as a whole by using questionnaires and on-site interviews, and specific recommendations were provided. Such performance evaluation not only helps to enhance the Board's oversight functions and operational efficiency, but may also serve as a reference for directors' remuneration standards. The evaluation results were publicly disclosed on the company's website[1].

Remuneration for top management includes cash, stock options and restricted stock awards. The characteristics of the industry and the nature of the company's business are taken into consideration when determining the ratio of bonus payout based on the short- term performance of top management and the time for payment of the variable part of remuneration. Furthermore, we believe that the ownership of company shares by the directors who hold senior management positions help align their interests and actions with the interests of shareholders; therefore, we formulated "Stock Ownership Guidelines" and updated minimum value of stock ownership in 2023. To enhance corporate governance and ensure the accountability of financial results, we also updated "Compensation Recoupment Policy" in 2023 by expanding the scope of the policy to reserve the right to cancel and require reimbursement of any variable compensation received by the top management to the extent permitted by applicable laws. These two important documents were publicly disclosed in our website[2].

Shareholder Rights and Interests

To ensure shareholders' rights of being fully informed of, participating in and making decisions over important matters of the company, we have actively responded to TWSE's promotion of corporate governance related measures. These measures include a candidate nomination system for Board member elections, an electronic voting system, case-by-case voting at shareholder meetings, and the disclosure of voting results on a case-by-case basis. The shareholders' meetings are held in an effective, legal and convenient way for shareholders to exercise their shareholders' rights, encouraging shareholders participation in corporate governance and thereby leading to improved attendance at shareholders' meetings.

Information Transparency

We place great emphasis on the stakeholders' right to know, and faithfully comply with applicable regulations regarding information disclosure in order to provide them with regular and timely information on company financial conditions and business operations, major internal documents, and corporate governance status, etc. through diversified channels. These channels include the company website, Market Observation Post System (MOPS), annual report, SEC Filing Form 20-F, ESG Report, quarterly earnings release, press conference and annual shareholders' meeting. To treat stakeholders equally, we concurrently disclose the information of the preceding matters in both Chinese and English. This not only establishes a smooth and effective communication channel, but also grasps the pulse of the market, economy, society and environment through feedback from stakeholders.

[1] For further details on 2025 Board Performance Evaluation Results, please refer to the company's website at https://ir.aseglobal.com/html/ir_board.php
[2] For more important documents related to the company, please refer to the company's website at https://ir.aseglobal.com/html/ir_doc.php

3.2 Economic Performance and Tax Governance

Tax Policy

ASEH believes that being an honest and responsible taxpayer will help foster economic growth, contribute to business sustainability, reinforce our business value and positively affect our business partners.

ASEH is committed to:

1. Complying not only with tax laws and regulations, but also the spirit of the law, including the relevant international standards as well as duly completing accurate tax filings and complying with all tax payments in all the countries in which we operate.
2. Accounting for short-term and long-term tax influences in business decisions-making process.
3. Being transparent and disclosing tax information in accordance with applicable regulations and reporting requirements.
4. Complying with relevant tax payment on all profits earned from business activities conducted in the relevant jurisdictions and ensuring intra-group transactions are conducted at arm's length.
5. Not relying on tax havens or exploiting tax structures as a method of tax avoidance and aggressive tax planning.
6. Constructing an appropriate mechanism to assess tax-related risks and potential impacts connected to our global operations and constantly enhancing our tax governance activities.
7. Developing mutually trustful and respectful relationships with tax authorities and having open and honest channels of communication.

Our tax policy was reviewed and approved by our chief financial officer. The company's accounting department is responsible for income tax filing, and obtains approvals of the appropriate level of authorization before filing.

Consistent with our core values, ASEH is committed to fully meeting tax obligations while also being financially responsible for the potential effects that tax payments might have on our business activities and being supportive of corporate innovation, research and development, reinvestment and sustainable investment initiatives in accordance to government policy. As a multinational corporation, ASEH's tax contribution is international in scope and covers a wide range of public tax systems around the world.

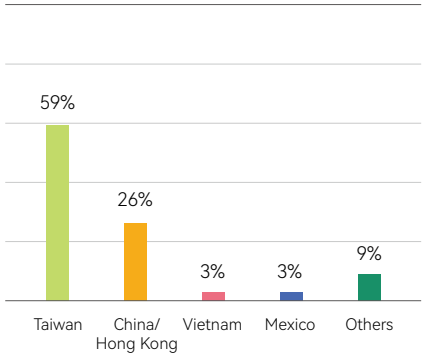
In view of the sophisticated nature of tax matters and the global scale that ASEH operates on, we continuously monitor and assess changes in relevant tax laws and regulations and implement internal training to ensure that employees have the necessary level of skill and awareness for tax issues. In addition to the internal training and guidance, we also have external tax advisors dedicated to advising us on material transactions and providing us with the foresight to mitigate the potential tax-associated risks. In addition to income tax, ASEH also contributes numerous other taxes including property tax, environmental tax and employment tax.

ASEH's global footprint spans across Asia, Americas, Europe, and Africa, covering more than 20 tax jurisdictions, with the principal offices and facilities located in Taiwan and China. Therefore, Taiwan and China contributed most of our operating revenues, profit before tax, income tax accrued for current year, and income tax paid. However, due to the variances in operating results and tax regulations among different tax jurisdictions, the proportions of net profit before tax, income tax accrued for current year and income tax paid may not be equivalent to the proportion of operating revenues. As for other individual countries where we operate, their proportions of the operating revenues, profit before tax and income tax accrued for current year, as well as income tax paid were relatively minor.

The bar charts below show the operating revenues, profit before tax, income tax accrued for current year, and income tax paid by country in 2025.

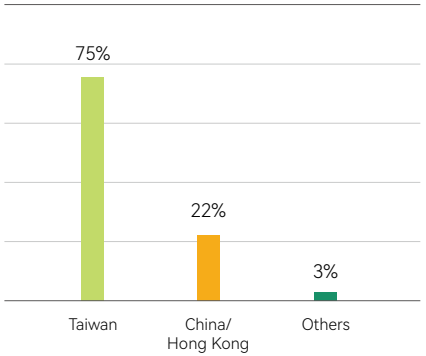
Operating Revenues

US$ 21 Billion
(NT$ 645 Billion)



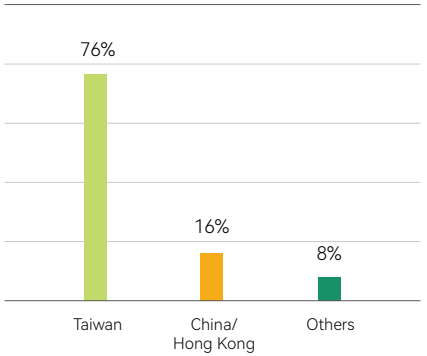
Profit (Loss) Before Tax

US$ 1,635 Million
(NT$ 51 Billion)



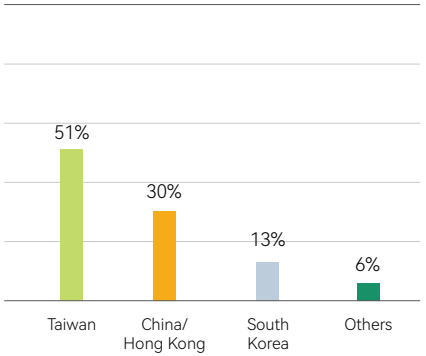
Income Tax Accrued

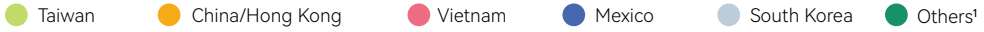
US$ 367 Million
(NT$ 12 Billion)



Income Tax Paid

US$ 227 Million
(NT$ 7 Billion)





In 2025, our effective income tax rate of 19.70% was higher than the industry average tax rate of 13.96% from SAM CSA Companion in "Semiconductors and Semiconductor Equipment" industry group. In Taiwan, the statutory income tax rate is 20.00% and the additional income tax rate on the unappropriated retained earnings ("URE") is 5.00%. Under IFRS, the URE tax should be recognized when profits earned; then in the following year, the company would do a tax adjustment of distribution of earnings. A slight increase of 0.73 percentage points compared to 2024 was primarily due to the impact of higher taxable income, withholding tax, URE, and Pillar Two income tax.

In 2025, our effective cash tax rate of 13.86% was higher than the industry average cash tax rate of 13.82%. A decrease of 10.68 percentage points compared to 2024 was mainly because one of our Cayman Islands subsidiaries paid the income tax for a gain from the disposal of our China subsidiaries in the previous year as the tax amount was confirmed in 2024.

[1] "Others" includes Singapore, Malaysia, Japan, the Philippines, U.S.A, Tunisia and European countries, etc.

3.3 Business Ethics

Policies and Specifications

The Board has successively approved and published ethical corporate management related regulations which clearly specify the policies and specification, behavior guidelines, operational procedures and grievance systems to prevent unethical behaviors. These policies aim to shape ASEH's culture of honesty and responsibility and to realize its commitment of compliance to the highest ethical standards in ASEH's overall business activities.

Organization and Authority

As the highest governance body of ASEH's business conduct and ethics, the CSISC coordinates and supervises the establishment and implementation of the ethical corporate management policies and specifications. The CSISC periodically reviews the promotion of business conduct and ethics and the compliance of policies and specifications, and reports to the Board on a yearly basis. The Corporate Governance Taskforce under the CSISC of the three major subgroups is established to promote ethical policies and specifications to our global manufacturing sites and assists in managing and adopting appropriate policies and specifications to ensure ethical management in compliance with the requirements of local laws and regulations. Global manufacturing sites are responsible for planning the internal organization, structure, and allocation of responsibilities, formulating standard operating procedures and conduct guidelines in accordance with corporate policies and specifications, and promoting awareness and educational activities with respect to ethics policy in internal management and in daily operation. The Group Internal Audit is in charge of supervision to ensure the operating effectiveness of reporting system, and reports to the Audit Committee regularly every year.

Ethical Related Regulations

- Code of Business Conduct and Ethics
- Corporate Governance Best Practice Principles
- Sustainable Development Best Practice Principles
- Ethical Corporate Management Best Practice Principles
- Procedure for Ethical Management and Guidelines for Conduct
- Administrative and Practice Procedures to Prevent Insider Trading
- Policy and Procedures for Complaints and Concerns Regarding Accounting, Internal Accounting Controls or Auditing Matters
- Fair Competition and Antitrust Laws Compliance Policy
- Guidance of Prevention of Corruption
- Procedures for Handling Whistleblowing Cases of Unethical Conduct
- Supplier Code of Conduct

Education and Promotion

To guide ASEH Members[1] and the company's stakeholders to better understand ASEH's business ethics standards, we set up "Code of Business Conduct and Ethics" area of the company website and disseminate our ethical related policies, guidelines, practices, and implementation status of the Board and management levels within the company. We also communicate ASEH's concept of business ethics and company's specific practices through education, promotion and online training and various methods, strengthening the culture of integrity in operation and ensuring the effective implementation of the system.

We require all suppliers to abide by the company's Code of Business Conduct and Ethics and Supplier Code of Conduct. In addition to the "ASEH Supplier Code of Conduct Commitment Letter" signed by new suppliers, relevant guidelines and regulations are specified clearly in our procurement documents and published on E-Hub, an electronic information exchange platform for suppliers. These steps are taken to ensure that all suppliers are cognizant of their obligations when conducting business with ASEH. Compliance with these codes is a prerequisite to qualify as an approved ASEH supplier. Over the years, we have organized annual supplier conferences and periodic workshops, forums, training sessions and monthly/quarterly/yearly appraisals to communicate with suppliers on our Supplier Code of Conduct, to ensure proper alignment in values and ethics.

[1] "ASEH Members" includes all employees, officers, supervisors and directors of the company, its subsidiaries and joint ventures

2025Programs and Implementation

Education and training, advocacy and communication:

1. The Administrative and Practice Procedures to Prevent Insider Trading of the company stipulate clearly the restrictions with regard to trading of shares by Board members. Email reminders on the policy and regulatory compliance were sent out by the corporate governance officer to the Board members prior to the blackout period when the Company released its quarterly and annual financial reports in 2025.
2. The company's Corporate Governance Officer has duly reported to the board on the company's current ethical management and work plans on May 12, 2025. The Board passed a partial amendment to the company's Guidance on Prevention of Corruption, Code of Business Conduct and Ethics, and Supplier Code of Conduct to enhance the protection of human rights, friendly workplace, and business ethics among ASEH entities and our global supply chain partners.
3. The company has promoted its business code of conduct and ethical compliance reporting mechanism on the Group Audit Management System platform, which is accessible to our global business locations. This is intended to help employees understand when and where they can file a report or complaint. We also conduct in-person information sessions with the management and employees at our global business locations to share selected case studies and procedures for handling reports of unethical conduct. We are continuously calibrating the reporting system to ensure ease of use and encourage proactive reporting on unethical behavior. We are committed to investigating and handling every report in a fair and equitable manner, in accordance with the company's whistleblowing policy.
4. ASEH's business locations around the globe have conducted business practices and ethics related training to all employees through In person and online training system to conduct, with the topics covered including ethical management, anti-corruption, trade secrets, fair competition, respect for intellectual property, prevention of insider trading, information security, RBA Code of Conduct, and employee code of conduct at all business locations (250,445 participants clocked a total of 205,841 hours on the course). In total, 54,672 employees attended the courses related to the company's Administrative and Practice Procedures to Prevent Insider Trading and on applicable laws and regulations.

Risk assessment:

- All of our sites around the world have conducted business ethics risk assessment and maintain existing control measures or develop corrective action plans based on the assessment results. No significant uncontrolled risks related to business ethics violations have been identified.

Consultation and Report

We have established channel of consultation for ASEH Members and various internal and external reporting channels[1]. ASEH Members or any third party may report to the internal or external channels, either using their own identity or anonymously. Investigation and improvements were made according to related reported issues, emphasizing on the importance of business ethics and integrity by providing educational training (such as e-mail advocacy and online quizzes). We are committed to keeping the whistleblower's identity and reporting contents confidential, and protecting him/ her from any unfair treatment or retaliation as a result of the violation reporting.

ASEH received a total of 138 complaints in 2025, of which 46 lack sufficient information to conduct further investigation or were employee-related complaints that have been forwarded to the HR department to follow up. There were a total of 70 complaints related to unethical business behavior. Of which, 44 cases pertaining to unethical business behavior were substantiated after thorough investigations were conducted, with 2 corruption or bribery cases, 1 conflict of interest case, and 41 discrimination or harassment cases. All necessary improvement measures have been taken, including taking disciplinary actions against violating employee, enhancing ASE members' awareness through trainings, conducting post-cases reviews to ensure the improvement measures taken to effectively prevent the recurrence of similar cases[2].

For the purpose to reinforce the whistle-blowing mechanism, the company has appointed an independent third party to assist in handling any reporting regarding insiders' misconducts in the course of investigation if necessary and provide legal services in the subsequent investigation since 2018.

[1] For further details on internal and external report channels, please refer to the company's website https://www.aseglobal.com/csr/integrity-and-accountability/business-conduct-ethics/
[2] For more detail on improvement measures related to harassment and discrimination, please refer to 6.1 Talent Attraction and Retention
[3] Number of cases lack sufficient information to conduct further investigation
[4] Number of cases involved employees' personal complaints and were forwarded to the HR department to handle
[5] Number of breaches confirmed related to ethics matters after investigation

Number of code of business conduct and ethics violation reports filed in 2025

Number of cases received: 138

Not accepted[3]	Not related to ethics matters[4]	Related to ethics matters
46	22	70

Item	Not Breach	Breach[5]
Corruption or Bribery	0	2
Conflict of Interest	1	1
Insider Trading	0	0
Money Laundering	0	0
Fair Competition and Antitrust	0	0
Secret Divulgence	0	0
Privacy and Personal Data Protection	0	0
Discrimination or Harassment	25	41
Total	**26**	**44**

Processing Procedures for Violation Reporting

1 **Filing**
Violation is reported.

2 **Acceptance**
Group Internal Audit accepts the report and conducts preliminary analysis.

3 **Investigation**
Audit Committee appoints chairperson of the investigation team, and an investigation team will be formed by the chairperson to select qualified personnel to conduct the investigation.

4 **Disciplinary and Corrective action**
Based on the investigation results, corresponding actions will be taken, including disciplinary actions, legal actions, corrective actions, and education and training.

5 **Reporting to Audit Committee**
Investigation team will forward an investigation report to Audit Committee via Group Internal Audit.

3.4 Risk Management

As a global company, managing risk is integral to ensuring business resilience and continuity. At ASEH, we have established a comprehensive risk management architecture in accordance with the Enterprise Risk Management (ERM) approach. In addition, we have incorporated the ISO 31000 Risk Management - Principles and Guidelines to manage risks in the day-to-day operations, together with systematic general risk control measures to form a comprehensive and effective risk management framework that also allows us to explore potential opportunities that may arise.

Risk Management Policies

The ASEH's Risk Management Policies and Procedures adopted by the board of directors in 2020, was designated as the highest level of foundation for the company's risk management. It explicitly mandates that risk management must be incorporated into both the company's business strategy and organizational culture, and that it is crucial to establish a comprehensive set of risk management procedures that undergo continuous review to ensure the effective control of risks.

Risk Governance Framework

The Governance level of Authority in Risk Management and Control – ASEH Board of Directors/ Risk Management Committee

As the highest decision-making authority of risk management and control, the board of directors of ASEH's. The members of the board have an extensive understanding of the industry landscape and experience in risk mitigation, to formulate risk management strategies that take into account both the company's business strategy and the overall environment. The Risk Management Committee, which consists of three independent directors, is a functional committee established directly under the board. The committee is responsible for overseeing comprehensive risk management, implementing risk management policies and decisions of the board, coordinating and promoting inter-departmental risk management plans, supervising and managing the company and its subsidiaries' risk management and control mechanisms, and reviewing and compiling risk management reports and submitting them to the board of directors on a regular basis.

The Third Line of Defense – Group Internal Audits

The Group Internal Audit (GIA) office was established under the board of directors to perform annual audits (at least once a year) of business operations and management processes related to risk management in order to evaluate the completeness of risk identification, the accuracy of risk assessment, and the implementation status of response measures in all departments. The goal is to ensure that all risks are effectively controlled within acceptable limits. The scope of the audit includes both the company and its subsidiaries, and the audit findings are presented to the board of directors to ensure objective oversight and management of various risks, as well as reasonable belief that the company's goals have been met.

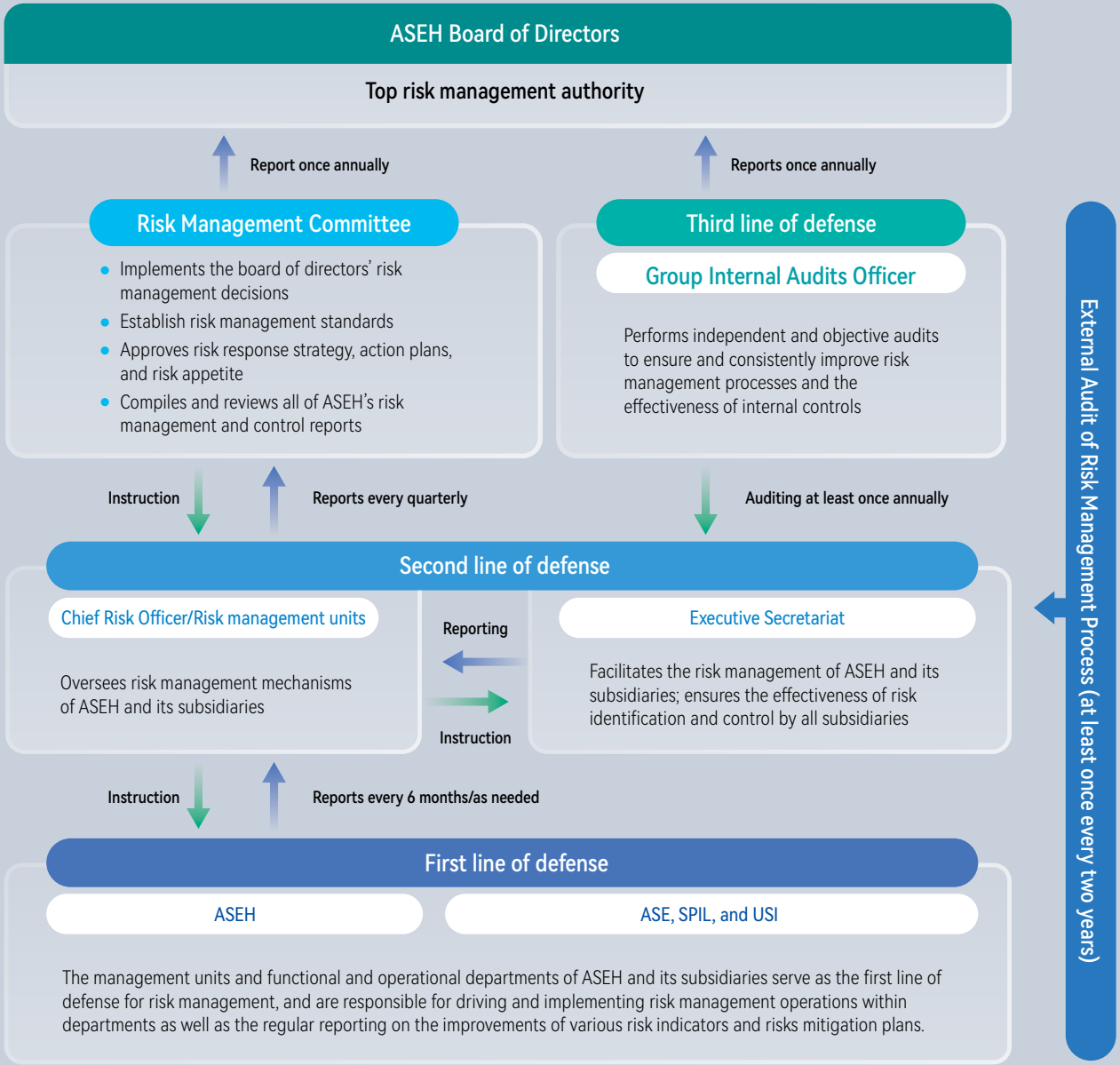
The Second Line of Defense - Chief Risk Officer

The board of directors has designated Du-Tsuen Uang, our Corporate Governance Officer, as the Chief Risk Officer. Uang's responsibilities include providing guidance and oversight for the risk management efforts of the company and its subsidiaries, and submitting annual reports to the Risk Management Committee. The Risk Management Executive Secretariat facilitates the implementation of risk management measures, while different functional units and subsidiaries undertake risk management tasks in accordance with their respective business needs and responsibilities.

The First Line of Defense – Responsibility of all functional units of ASEH and its Subsidiaries

The successful implementation of risk management is contingent upon the integration of risk management principles into the day-to-day activities of all employees across the company. The company outlines the roles and responsibilities of the functional units and each unit is accountable for the risks arising from the day-to-day operations. We will continuously promote a corporate culture of risk awareness across the company to enable our employees to better understand, identify and manage associated risks. Furthermore, in order to effectively manage and control overall company risks, our subsidiaries are required to establish risk management committees that report to the Chief Risk Officer and Risk Management Committee.

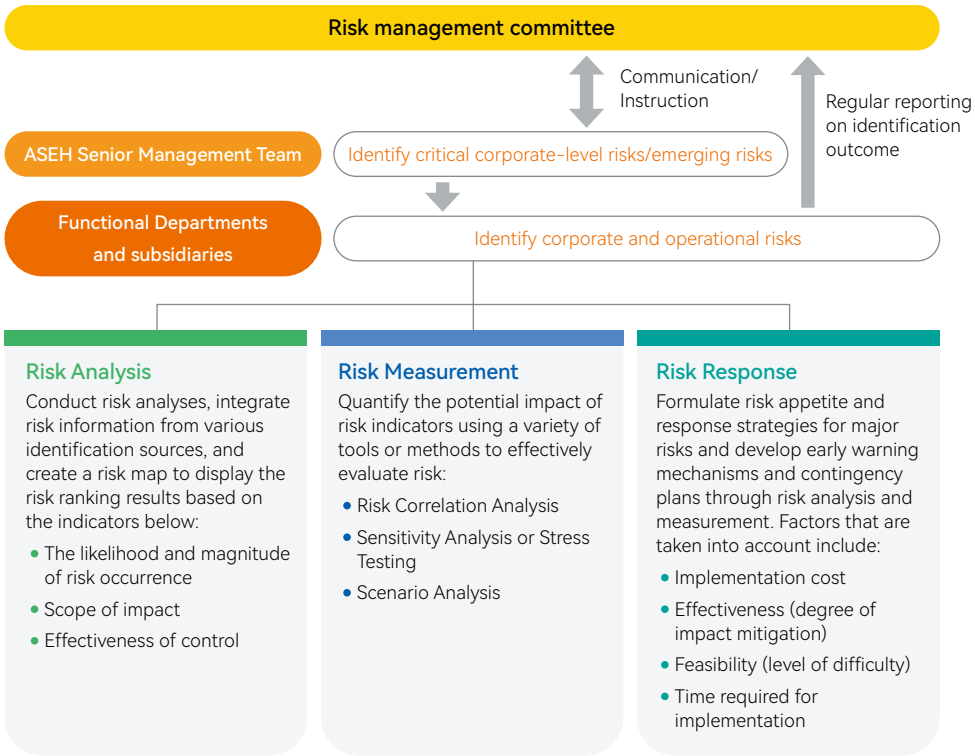
Risk Governance Framework



Risk Identification Process

ASEH implements a top-down ERM approach to identify effectively critical operational and strategic risks. Each year, the senior management team meets to identify potential risks, while a bottom-up risk inventory mechanism is employed to identify corporate-level and operational-level risks in all subsidiaries. The risks identified by the senior management team and the risk management of each functional unit are integrated to form a comprehensive risk identification process. The identified risks are documented in the Risk Register and subject to evaluation to identify the key risks according to risk level and control effectiveness, and subsequently, to develop a risk response strategy or risk management plan accordingly. To clarify potential correlations between various risk factors, we employ the Correlation Analysis method to analyze them, formulate risk mitigation plans in the event that relevant impacts are found, and regularly monitor the implementation status and effectiveness to reduce t residual risks.

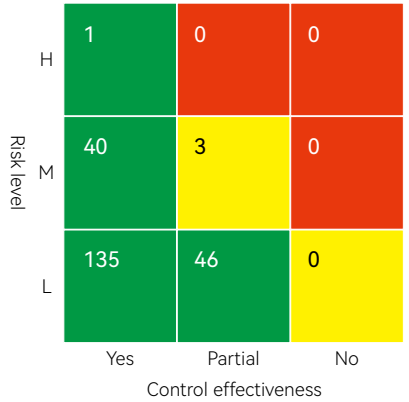
Risk Identification Process



Risk Analysis

The functional risk management units identify potential risks encountered in their day-to-day operations and rank them using indicators such as the probability of occurrence, level of impacts, and control effectiveness. In 2025, the company identified a total of 225 risks from its annual risk identification and analysis. The distribution of the associated risk levels is indicated as follows:

ASEH Risk Matrix



Risk Measurement

Based on the results of the risk analysis, we perform annual risk measurement on major risk factors. Depending on the attributes of the risk factors, we then employ a variety of methods and tools, including Risk Correlation Analysis, Sensitivity Analysis or Stress Testing, and Scenario Analysis, to assess the impact of risks on the company or correlations between risks. This evaluation also determines whether it is necessary to adjust the level of risk appetite or tolerance.

Risk Category	Risk Description	Measurement Methods/Tools
U.S. BIS Export Control Risk	Enterprises complying with U.S. BIS regulations by imposing restrictions on customers in specific regions may run afoul of other countries' laws—such as China's Anti-Foreign Sanctions Law or Unreliable Entity List provisions—thereby facing a dual risk of being sanctioned, sued, fined, or having their assets frozen in that market.	Scenario Analysis、Sensitivity Analysis、Stress Testing Sensitivity Analysis
Interest Rate and Foreign Exchange (FX) Risk	Interest rate risk refers to the risk that the company's annual interest expense will increase in response to a 100-basis-point (1%) rise or fall in the benchmark interest rate. Exchange rate risk refers to the impact on the company's net profit or shareholders' equity, all else being equal, in response to a depreciation or appreciation of the New Taiwan Dollar (NT$) against the U.S. Dollar (US$).	Sensitivity Analysis、Stress Testing
Supply chain risks	The risk of material supply disruption due to the potential shutdown of suppliers' production bases or port closures resulting from an unexpected outbreak of war.	Sensitivity Analysis、Stress Testing

Decision-making Process for Risk Tolerance and Response Strategies

After the risk factors have been identified and measured, the Chief Risk Officer, who serves as the second line of defense in the organization's risk management, is responsible for collating the proposed risk tolerance and response strategies before reporting the summary to the Risk Management Committee. The Risk Management Committee will then review and decide on the proposed risk tolerance and response strategies, and submit to the board of directors for their reference and subsequent execution. This entire process provides a firm basis for the implementation of risk control and response measures.

Risk Response Measures

Geopolitics, Energy management and renewable energy risks, as well as Cyber Security risks, are among the primary risks for ASEH in 2025. The company's risk tolerance and mitigation measures were planned in accordance with the findings of the comprehensive risk assessment.

Three Lines of Defense for Risk Management

	ASEH and functional units of subsidiaries	Chief Risk Officer	Risk Management Committee
Decision-making process for risk tolerance and response strategies	Identify potential risk impacts	Verify risk tolerance and formulate response strategies	Determine risk tolerance and response strategies
Management process for risk tolerance and response strategies	Regular review of various risks and their control points	Verify the risks that are subject to routine monitoring	Continuously monitor the effectiveness of risk management

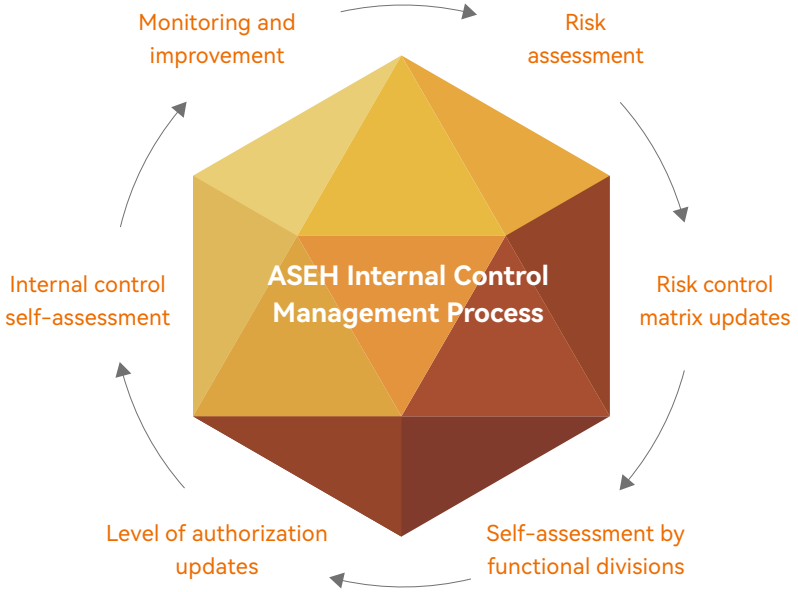
Risk Category	Risk Description	Mitigation Measures
Geopolitics	When enterprises implement restrictions on customers in specific regions in order to comply with U.S. BIS (Bureau of Industry and Security) regulations, they may inadvertently violate other countries' laws—such as China's Anti-Foreign Sanctions Law or Provisions on the Unreliable Entity List—thereby exposing themselves to a dual risk of sanctions, litigation, fines, or asset seizure within that market.	1. Taking the US-China trade restrictions as an example, the company should have its legal department identify the impact of regulatory changes, senior management decide on countermeasures, procurement and sales departments assess the scope of restrictions, IT update system settings to manage risk, and continuously monitor regulatory changes to minimize losses. 2. Strengthen global layout 3. Actively cultivate local suppliers to achieve short-chain supply 4. The original production site dispatches experts to go overseas to train local personnel
Energy management and renewable energy risks	Energy regulations and energy efficiency standards (such as minimum energy performance standards for motors and air conditioners) are continually being raised. Enterprises that fail to upgrade their equipment in a timely manner may face fines or forced suspension of operations. In addition, renewable energy developers (power plants) may be unable to deliver electricity as scheduled due to natural disasters, project delays, or financial difficulties, resulting in a green power supply gap for enterprises.	1. Continuously monitor changes in energy regulations across regions. 2. Implement an AI-based smart energy management system to enable precise data monitoring, and prioritize "energy-saving technology upgrades" (which offer the lowest cost and most direct benefits). 3. Adopt a diversified strategy (such as installing self-built rooftop solar systems combined with signing medium- to long-term green power procurement agreements, i.e., CPPAs) to mitigate the risk of relying on a single supplier.
Cyber Security Management	Attackers are leveraging AI to rapidly generate ransomware variants without malicious signatures, or to automatically identify and screen enterprise vulnerabilities, causing both the frequency and precision of attacks to increase exponentially. In addition, AI is being used to impersonate the voice or image of corporate senior executives to carry out precisely targeted "Business Email Compromise (BEC)" scams, deceiving finance personnel into transferring funds or disclosing critical credentials.	1. Continuous cybersecurity education and training and irregular phishing drills 2. Implement two-factor authentication 3. Perform system vulnerability scans regularly 4. Purchase information security insurance

Verifying the Effectiveness of Risk Management

Internal Control

ASEH's Internal Control Policy complies with the Regulations Governing Establishment of Internal Control Systems by Public Companies established by Taiwan's Financial Supervisory Commission (FSC) and the pertinent regulations of the U.S. Securities and Exchange Commission. The policy, developed by senior management and approved by the board of directors, encompasses control operations at the corporate and operational levels. The objective is to establish a scope and standards that are applicable to the internal control systems of all of the company's business units and subsidiaries, thereby achieving effective design and implementation of internal controls, promoting the sound operation of the company, and to reasonably ensure accomplishment of the following objectives:

- Operational efficiency and effectiveness
- Transparency, reliability, timeliness, and legal compliance in reporting
- Compliance with the relevant laws and regulations



Risk-based Internal Audits

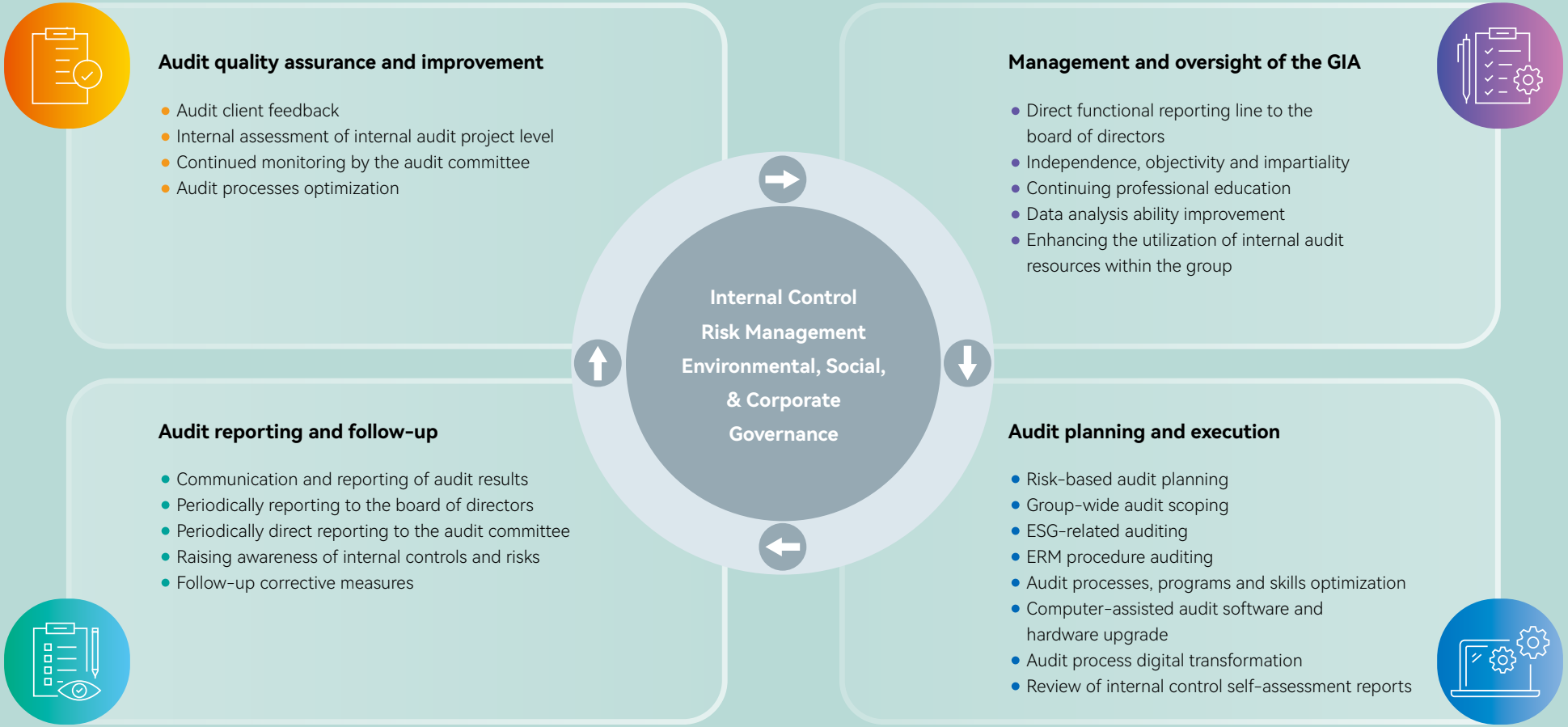
The Group Internal Audit (GIA) office was established under the board of directors to assist the board and management in reviewing and evaluating the effectiveness of the internal control system, measuring the effectiveness and efficiency of the company's operations, and assessing the reliability, timeliness, transparency, and legal compliance of relevant reports. In addition, the GIA office makes timely recommendations for improvements to reasonably ensure the continuous operating effectiveness of the internal control system, and to provide a basis for reviewing and revising the internal control system.

The GIA Division comprises an internal audit officer and an appropriate number of qualified, dedicated internal auditors as indicated by business scale, operating conditions, management needs, and the provisions of applicable laws and regulations, to perform independent, objective audits. Besides possessing competent qualifications, internal auditors are required to enhance their audit expertise by undergoing continuous skills training on an annual basis. The GIA team is fully dedicated to enhancing the company's audit programs, procedures, and techniques, and developing audit tools to improve internal audit efficiency and effectiveness.

The GIA office utilizes a risk-based internal audit mechanism and performs internal audit activities in accordance with the annual audit plan approved by the board of directors. The scope of the internal audit includes the internal control systems of the company and its subsidiaries. By integrating audits with our corporate risk management strategies and practices, and conduct independent audits on risk management business activities and processes in accordance with the ISO 31000 Risk Management Framework. This involves reviewing whether risk identification across units is comprehensive, risk assessments are accurate, and risk responses are effectively implemented, thereby ensuring all risks are controlled within tolerable limits. An annual Risk Management Audit Report is issued to the Chief Risk Officer (CRO) and submitted to the Audit Committee. For 2025, the Audit Report on Risk Management Policy and Procedures was signed and approved by the CRO on June 3 and submitted to the Audit Committee on June 27. By evaluating the response and continuous improvement mechanism (PDCA) of risk governance, the oversight function is effectively fulfilled.

The internal control self-assessment reports, prepared by the company and its subsidiaries and reviewed by the GIA office on an annual basis, along with audit reports on findings of internal control system deficiencies and abnormalities identified by the GIA office serve as the primary basis for the board of directors and general manager to assess the overall effectiveness of the internal control system and to produce internal control system statements.

Internal Audit Management Process

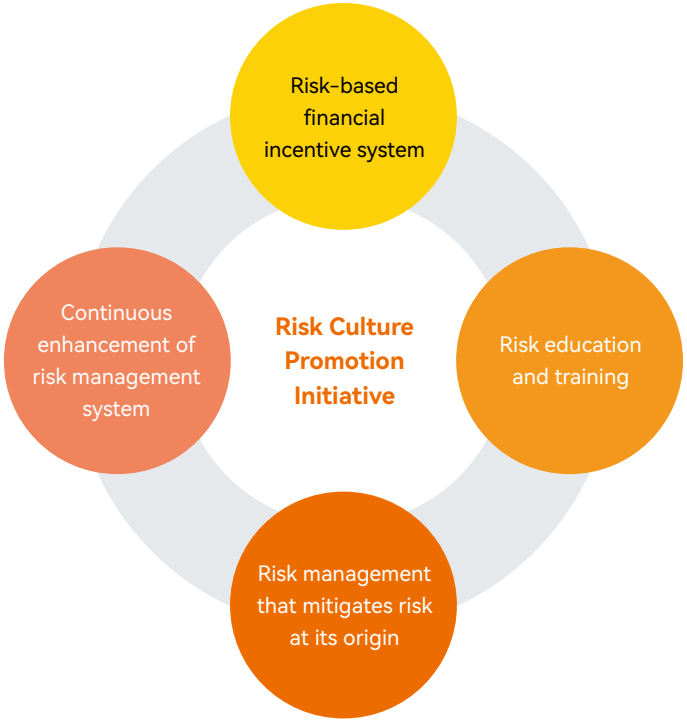


External Third-party Audit Verification

ASEH maintains major operating bases throughout the globe to ensure that its customers receive the most comprehensive and timely service possible. In light of the evolving business landscape, we have introduced annual external risk management process audits by third-party organizations in addition to establishing rigorous internal audits and internal control systems. In addition to ensuring the effective implementation of the company's risk management processes, we also annually review the operation of relevant systems by referencing feedback from internal and external audit results. This continuous review aims to deepen and enhance the effectiveness of our risk management. BSI Taiwan was appointed to verify the ASEH risk management system in accordance with the ISO 31000 Risk Management - Principles and Guidelines, ensuring that the company's risk management is in compliance with international standards, and demonstrating conformity.

Promoting a Risk Culture

Successful risk management requires a comprehensive and robust risk management structure, and a deep-rooted sense of risk awareness among all employees. To that end, ASEH has formulated a plan to promote corporate risk culture and implement initiatives across all levels of the company. Our objective is to gradually cultivate a shared understanding of risk management with employees, enabling them to identify potential risks and respond effectively to mitigate the company's overall risk.



Risk-based Financial Incentive System

ASEH believes that risk management requires active involvement from all levels of the company, especially from our employees. The ASEH Corporate Sustainability and Information Security Committee (CSISC) plays an active role in strengthening employee focus on risk management. The CSC is composed of members from the board of directors and the senior management, and is chaired by the Board Chairman. The CSC is responsible for overseeing various projects and reporting their implementation status to the Board, with the goal of balancing business growth with generating positive social and environmental impacts. The CSISC presents the Board with a report at least once a year that addresses the following topics: (1) the status of sustainability development; (2) current policies, regulations, and organization; and (3) management policies, objectives, and future plans for material sustainability issues. The Board also supervises the implementation of the policies and evaluates the progress made.

The ASEH Corporate Sustainability Division functions as the executive secretariat of the CSISC, assisting in the coordination and consolidation of resources and functional teams from our three main subsidiaries to drive sustainability through a comprehensive and interconnected strategy. At each subsidiary level – ASE, SPIL and USI have formed their respective corporate sustainability committee with multiple task forces. These task forces are led by the senior management team who meet regularly to discuss pertinent issues, highlight annual accomplishments and outcomes, and evaluate the advancement of short, intermediate, and long-term sustainability objectives. We have designed a compensation program (via the allocation of restricted stock options) that links the achievement of specific risk objectives and the Annual Objective Deployment (AOD) to individual performance evaluation. At USI, the management employs the Golden Circle concept whereby risk factors that may have a significant impact on operations and production are analyzed and monitored. The company then rewards business units that have demonstrated effective risk control. On the other hand, In 2025, ASE Kaohsiung launched its inaugural ESG Awards. The event integrated energy conservation, carbon reduction, energy risk management, and safety risk management into competitive activities, offering direct financial incentives to units demonstrating outstanding energy-saving performance.

As part of this initiative, the Fire Safety Challenge featured interactive scenarios covering fire safety, medical response, and emergency preparedness, reinforcing employees' awareness of occupational health and safety risks through practical operations. The competition included four categories—Team, Individual, Women's, and Overseas:

- **Team Category:** Awarded NT$10,000 for 1st place, NT$8,000 for 2nd place, and NT$5,000 for 3rd place.
- **Individual Category:** Awarded NT$5,000 for 1st place, NT$3,000 for 2nd place, and NT$2,000 for 3rd place.
- **Women's and Overseas Categories:** Awarded NT$8,000 to the 1st place winners in each category.

Risk Education and Training

ASEH adopts a dual-prong top-down and bottom-up approach to risk management. The company continues to enhance the management's awareness of risk management and places great emphasis on demonstrating exemplary leadership from the corporate governance levels in risk management to drive risk awareness, and inculcate a strong risk culture across all levels in the organization.

Risk Education and Training for Board Members

On an annual basis, board members undergo a series of industry-curated training programs that are structured according to their academic and professional background. In 2025, with reference to international trend developments and the Company's risk assessment results, the Directors will be arranged to attend courses on risk management topics such as "Strengthening Regulatory Compliance to Ensure Sustainable Operations Course" and "Deciphering the Trump Administration's Economic and Trade Strategies", as well as regular corporate risk management-related courses such as "Enterprise Risk Management and Major Risk Development Trends".

Risk Education and Training for All Employees

We also provide internal training courses that are crucial to risk management. In addition to conducting ERM and BCM work forums to increase the risk awareness of senior managers, we have also organized a variety of courses that have achieved 100% participation rate, for all employees. In 2025, a total of 36 courses were conducted across the entire company, classified into 5 major categories, the courses have attracted 371,940 participants, and all employees have completed relevant risk training.

2025 Risk-related Education and Training

Course Title	Targeted Trainees	Number of Participants	Completion Rate	Training Hours
Product Safety	Technical positions	47,944	100%	2
Legal Compliance	Managerial, technical, and administrative positions	45,041	100%	1.5
Risk Management	All employees	92,985	100%	1
Information Security Awareness	All employees	92,985	100%	1.5
Environment, Health, and Safety	All employees	92,985	100%	2.5

Risk Prevention from the Source

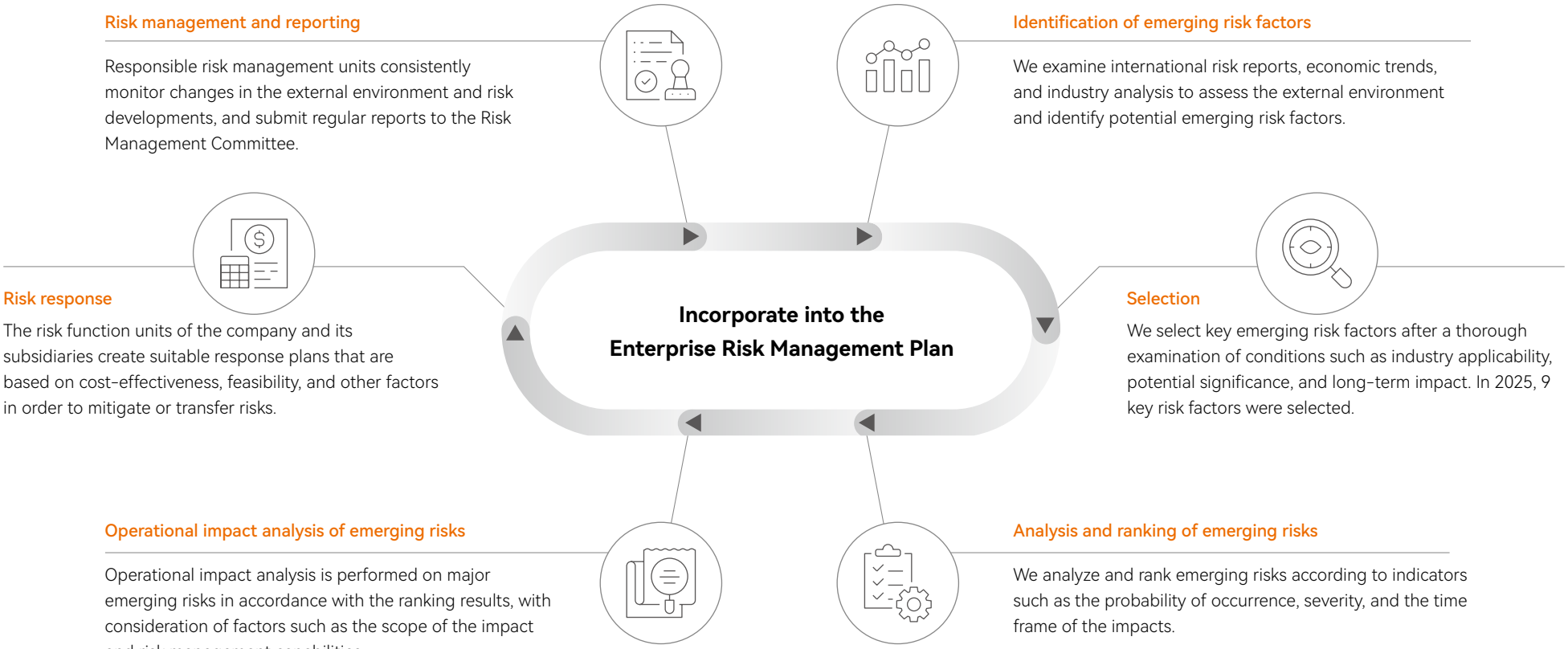
As the saying goes 'prevention is better than the cure', we believe that measures and actions taken in advance help eliminate the threat of risks. We have incorporated risk criteria into the initial development stage and throughout the approval processes of our products and services. For instance, we implemented a product quality assurance system that accounts for risks related to the market, intellectual property, finance, technical feasibility, and other factors in the planning phase. In the subsequent manufacturing process, we select lower-risk raw materials, improve quality and reliability, and facilitate the continuous improvement of overall production yield standards through a sound and comprehensive planning system.

Continuous Improvements of the risk management system

To reinforce our risk management practices, we have adopted measures that enable individual employees to proactively identify and report potential risks, as well as encourage employee participation through a structured feedback process. ASEH's subsidiaries have all successfully completed ISO 9001, ISO 14001, and ISO 45001 and other relevant certifications. Continuous improvements to the risk management process is further enhanced by applying the techniques in the Plan, Do, Check, and Act (PCDA) cycle that effectively triggers a wide range of potential risks for immediate attention. All risks are assessed and managed within the institutionalized settings, while risk responses are incorporated into standard management procedures through the internal management communication system. The company's primary operating bases have all obtained ISO 22301-Business Continuity Management certification.

Long Emerging Risks

From the rapidly evolving business environment, to ongoing technological breakthroughs and escalating deglobalization, a multitude of global developments have elevated uncertainties that directly affect ASEH's operations. It is therefore crucial for the company to fully understand the potential impacts of external emerging risks on ASEH's key businesses. The company identifies key emerging risk topics through a risk identification and analysis framework, and reviews potential risk mitigation and response measures rigorously to strengthen its capacity to adapt to external change. At this point, it is challenging to quantify emerging risks due to their forward-looking nature, and it is probable that they will develop into substantial risks in the future. Therefore, we have established a systematic emerging risk identification and assessment process to prepare for emerging risks in the future, and to assist the board of directors and senior management in making decisions that align with our business strategies and long-term value.



Based on the aforementioned process, ASEH has identified the following key emerging risks and the corresponding monitoring and control mechanisms:

Type of Risk	Description	Potential Impacts	Response Measures
Risk of Unannounced Warfare/ Geopolitical Conflict	An internationally unanticipated outbreak of war (or armed conflict) generally refers to a conflict that erupts within a short period of time—often due to the failure of diplomatic negotiations, intelligence misjudgment, or a surprise offensive strategy adopted by one party—causing significant shocks to the international order. If critical shipping routes were to be blockaded, it would disrupt global energy transportation, affecting not only gasoline and diesel prices but also severely impacting the transport of petrochemical intermediates, industrial equipment, and daily necessities, thereby causing supply chain disruptions.	1. **Critical Component "Shortage/Mismatch" Crisis:** If even a single critical component (such as specialty gases, specialty steel, or patented control chips) originates from a conflict zone, the entire production line can come to an immediate halt. 2. **Spiraling Cost Increases:** Competition for alternative components and rerouted logistics costs will erode profit margins, while volatile energy prices will drive operating costs out of control. 3. **Contract Breach and Trust Crisis:** Delivery delays to downstream customers may trigger legal disputes, and could even lead customers to permanently shift to competitors in other geographic regions after the conflict ends.	1. **Geographic Diversification of the Supply Chain (China/Area + 1 Strategy)** **Decentralization:** Conduct a comprehensive review of the existing supply chain to avoid regions with heightened geopolitical tensions. Promote "near-shoring" by dispersing production bases to countries with stable political positions and complementary capabilities. Establish clear visibility over Tier 1 suppliers, as well as the geographic distribution of Tier 2 and Tier 3 suppliers. 2. **Strategic Buffer Inventory and Alternative Solutions** **Critical Material Reserves:** For materials that are "single-sourced" and irreplaceable, establish a safety stock of 6–12 months or more, rather than relying on traditional Just-in-Time (JIT) practices. **R&D Involvement:** Promote "design-out" strategies by incorporating multiple material options at the product development stage, ensuring that specifications can be quickly switched in the event of war. 3. **Establishment of a "Wartime" Crisis Task Force** **Scenario Simulation Drills:** Conduct regular "war gaming" exercises to simulate the company's contingency response procedures in the event that specific critical shipping routes or supplier countries become unavailable. **Digital Resilience Building:** Strengthen the supply chain visibility system (Control Tower) to ensure real-time tracking of the location and status of all materials at the first sign of disruption.
New Forms of Digital Threats and Cybersecurity Risks	Attackers are leveraging AI to rapidly generate ransomware variants without malicious signatures, or to automatically identify and screen enterprise vulnerabilities, causing both the frequency and precision of attacks to increase exponentially. In addition, AI is being used to impersonate the voice or image of corporate senior executives to carry out precisely targeted "Business Email Compromise (BEC)" scams, deceiving finance personnel into transferring funds or disclosing critical credentials.	1. **High Ransom Payments and Operational Downtime Losses:** Once an OT (Operational Technology) production line is targeted by ransomware, a single day of downtime can result in losses of millions of dollars, along with the devastating risk of unrecoverable data loss. 2. **Core Technology Leakage:** Hackers may infiltrate systems for months or even years through APTs (Advanced Persistent Threats), stealing core process parameters, undisclosed source code, or proprietary designs. 3. **Trust Crisis:** Leakage of customers' and partners' personal data can lead to serious legal litigation, substantial regulatory fines, and irreparable damage to corporate reputation. 4. As cybersecurity regulations become increasingly stringent worldwide (such as Taiwan's Cyber Security Management Act, the EU's NIS 2 Directive, and new SEC cybersecurity rules in the United States), enterprises that fail to fulfill their cybersecurity protection obligations may expose management to legal liability and penalties.	1. **Implement a "Zero Trust" Architecture:** Follow the principle of "never trust, always verify." Whether the user or device is inside or outside the corporate network, access to any resource must undergo strict identity verification, device health checks, and least-privilege authorization, thereby eliminating opportunities for hackers to move laterally once they penetrate the internal network. 2. **Joint Defense Mechanisms and AI-Powered Cybersecurity (Defense in Depth):** **Fighting AI with AI:** Deploy EDR (Endpoint Detection and Response) and XDR (Extended Detection and Response) systems, using machine learning to analyze abnormal behavior in real time (such as an employee account downloading large volumes of data at unusual hours) and automatically block threats before they escalate. **Threat Intelligence Sharing:** Join industry cybersecurity information sharing and analysis centers (such as ISACs) to obtain the latest vulnerability and blacklist intelligence in real time, enabling proactive defense. **Strengthening Digital Resilience and Supply Chain Governance:** Establish "Shadow AI" and Third-Party Security Management: Strictly control employees from inputting sensitive company data into unauthorized external AI tools, while also incorporating cybersecurity assessments into supplier contracts. 3. **Implement Multi-Track Backups and Drills:** Apply the "3-2-1 backup rule" (3 copies of data, 2 different media types, 1 off-site/cloud immutable backup), and regularly conduct "red team-blue team" simulation exercises to ensure rapid recovery in the event of a breach.

Type of Risk	Description	Potential Impacts	Response Measures
Risk of Rapid AI Technology Development	With the rapid development of artificial intelligence (AI) technology, enterprises often incur "technical debt" when implementing AI solutions due to a focus on speed, resulting in significantly higher costs down the road. AI technical debt is a critical yet frequently overlooked aspect of the AI development process; in essence, it refers to shortcuts taken for the sake of convenience in the present, which ultimately must be repaid as future costs.	AI technical debt can manifest in forms such as complex, unmanageable code, as well as a lack of version control for models and data. In the pursuit of quick fixes, enterprises often neglect fundamental, long-term solutions and adopt the wrong AI technologies, significantly increasing the difficulty of subsequent maintenance and upgrades. This creates the risk of an unpredictable surge in operating costs.	Strengthening the Precision Assessment of AI Technology Selection 1. **Root Cause Analysis (RCA):** When facing operational issues, enterprises should first conduct an in-depth diagnosis of pain points, rather than blindly following the latest and most expensive large models that may not necessarily be suitable for their needs. 2. **Cost-Benefit Analysis (CBA):** A full lifecycle cost estimate—including computing power, storage, maintenance, and potential technical debt cleanup expenses—should be conducted at the outset of implementation, rather than focusing solely on first-year development costs, in order to prevent subsequent cost surges.
Green Transition Risk	As governments and enterprises pursue carbon neutrality, implement carbon pricing, and adjust energy structures and regulatory compliance, immature carbon capture technologies, uneven distribution of green energy, supply chain gaps, and inconsistent pacing of regulatory compliance can lead to a sharp increase in production costs, resulting in "greenflation." In addition, key low-carbon raw materials required for the transition (such as copper, lithium, nickel, or renewable energy equipment) face short-term supply-demand imbalances, while carbon-intensive industries are subject to carbon fees—together driving up production costs across the overall economic system, either permanently or in stages.	1. **Technology Transition Failure:** If an enterprise rashly invests in low-carbon technologies that are not yet fully commercialized, and the R&D outcomes fall short of expectations or the supporting infrastructure (such as green power or hydrogen supply) remains immature, it may face severe investment losses. 2. **Greenwashing Allegations:** If an enterprise's carbon footprint disclosures or Scope 3 emissions inventories lack transparency or accuracy, any audit findings revealing delays or inaccuracies could result in reputational damage, legal litigation, and even direct removal from the supply chains of major international corporations.	1. **Diversification of Green Energy Assets and Supply Chain Defense:** Through green power purchase agreements (PPAs), investments in microgrids, or the deployment of distributed renewable energy, enterprises can avoid over-reliance on a single traditional energy source or a single green power supplier. Amid the price pressures caused by greenflation, locking in long-term energy costs helps ensure operational continuity. 2. **Implementation of a "Digital Carbon Management and Inventory System":** Leveraging AI and Internet of Things (IoT) technologies to precisely and automatically account for enterprise Scope 1, 2, and 3 carbon footprints, and integrating carbon data with financial reporting. With scientifically grounded and transparent data, enterprises can effectively meet Taiwan's sustainability regulations and international compliance requirements, thereby thoroughly eliminating the legal and reputational risks associated with "greenwashing.".
Reclaimed Water Resources Management Risk	The company faces uncertainty in Reclaimed Water Resources regulations, making it difficult to assess investment costs and risks, which results in unpredictable compliance risks and expenditures.	1. **Capital Allocation and Investment Assessment Challenges:** Changes in the scope of policies and standards increase the complexity of estimating water-related capital expenditures (CAPEX) and return on investment (ROI). 2. **Operating Cost (OPEX) Volatility Risk:** Future adjustments to water tariff structures, the imposition of water consumption fees, or potential compliance penalties may increase uncertainty in overall operating costs. 3. **Administrative Review and Plant Construction Timeline:** Adjustments to water-related environmental impact assessment and water rights review standards may increase the administrative communication costs and lead time required for new plant construction or capacity expansion projects.	1. Invest in a Reclaimed Water Plant to Reduce Water Consumption 2. Enhance the Treatment Efficiency of the Reclaimed Water Plant 3. Implement Water-Saving Improvements (Wastewater Recycling and Source Reduction) 4. Introduce New Water-Saving Technologies, Equipment, and Materials (1) Facility Operations: Recover chemically treated wastewater and reintroduce it into the production process. (2) Process Operations: Evaluate the use of water-efficient equipment or optimize water usage processes to achieve source-level water reduction.

3.5 Human Rights Management

Human Rights Policy

ASEH is committed to safeguarding the human rights of employees and value chain partners (including customers, suppliers/contractors, agents, joint ventures and consortia partners and local communities) and promoting the sustainable development of the environment, society and economy. ASEH complies with the legal and regulatory requirements of all operational locations and the approach is designed in support of the United Nations Universal Declaration of Human Rights (“UDHR”), the UN Global Compact (“UNGC”), the UN Guiding Principles on Business and Human Rights (“UNPBHR”), ILO Declaration on Fundamental Principles and Rights at Work(“ILO”), OECD Due Diligence Guidance for Responsible Business Conduct(“RBC”), Responsible Business Alliance Code of Conduct(“RBA”) and Corporate Sustainability Due Diligence Directive (“CSDDD”). ASEH is also committed to upholding local laws and regulations in the countries where ASEH operates, and reviewing the implementation of its human rights policies on a regular basis through membership on the Responsible Business Alliance.

Commitment

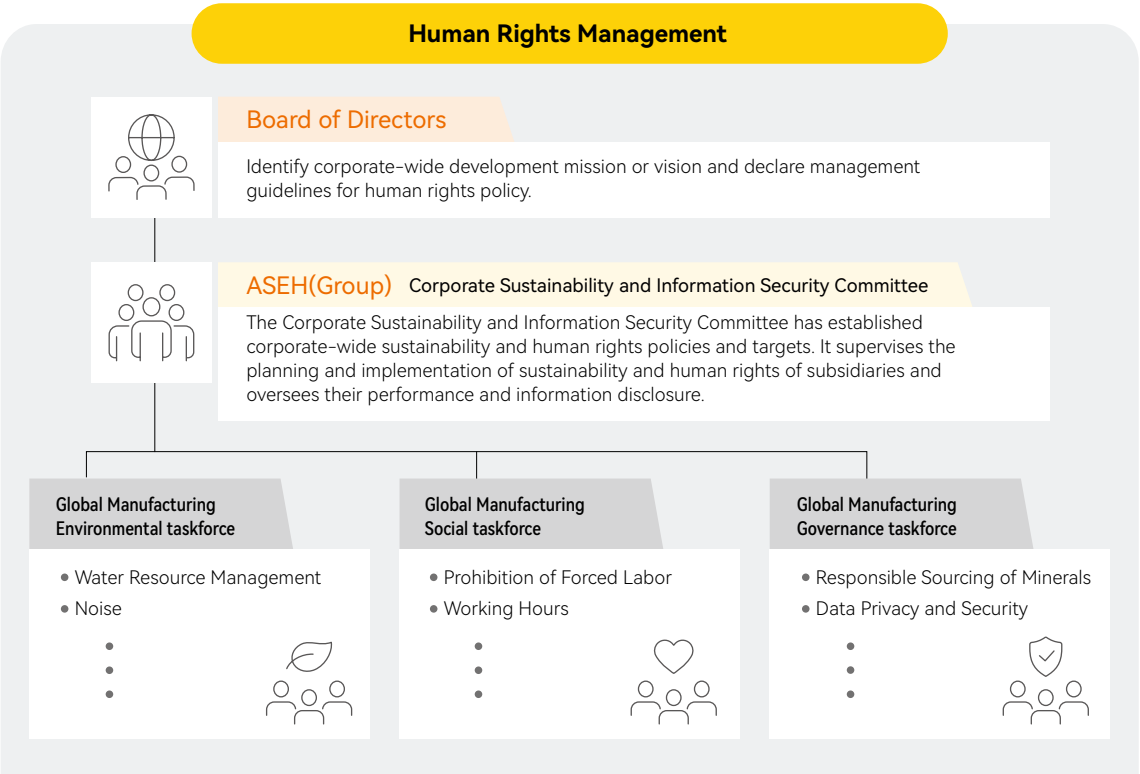
- Protection and Respect: ASEH is committed to protecting and respecting human rights and creating an environment conducive to human rights protection. ASEH strives to prevent any business activities that might result in human rights violations or adverse impacts.
- Appeal and Remedy Process: To protect the human rights of ASEH employees and value chain partners from violations or negative impacts, ASEH ensures that they have the right to raise concerns, report issues, or file complaints regarding suspected human rights infringements. ASEH also provides remedial actions and implements safeguards to prevent retaliation or unfair treatment against those who file complaints.
- Management and Investigation: ASEH seeks to continuously improve human rights governance with education and training and human rights due diligence and feedback mechanism. These efforts aim to integrate human rights management and policies throughout ASEH’s operations and partnerships across the value chain.

Management Organization

In order to adequately manage human rights issues that arise from operating a global business, ASEH implements risk management at all facilities, collates and reports the information to the ASEH Corporate Sustainability and Information Security Committee and top management at regular meetings.

Guidelines of Management

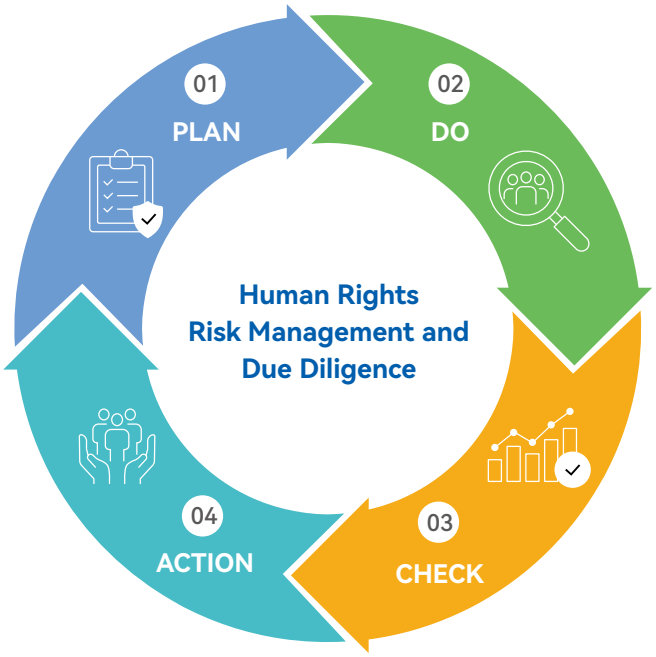
ASEH has adopted human rights management practices that follow PDCA management procedures and include risk identification, assessment, monitoring, control, and disclosure. In a reflection of the different roles played by ASEH, we focused our human rights management efforts primarily on employees of our own operations and joint ventures, suppliers/contractors, local communities, and customers. Through various due diligence processes and grievance mechanisms, we conduct human rights impact assessments to identify its salient human rights issues and develop appropriate mitigation and remediation measures to minimize the risks and impacts of potential human rights incidents.



Risk Management and Due Diligence

To fulfill its responsibility to respect human rights, ASEH has established a Human Rights Policy and Human Rights Management Framework, implementing its commitment to respecting, protecting, and upholding human rights. In doing so, it references the EU Corporate Sustainability Due Diligence Directive (CSDDD) and the OECD Due Diligence Guidance for Responsible Business Conduct to establish a due diligence process. Through the PDCA approach, ASEH regularly conducts human rights due diligence to assess and identify adverse impacts on human rights and the environment ("human rights risks"). For identified salient risks or incidents of human rights violations, it proactively develops and implements appropriate mitigation or remedial measures and integrates them into its business operations and management processes. Furthermore, ASEH has established a grievance management mechanism and provides independent and confidential grievance channels to investigate, process, and implement necessary remediation for grievance cases. By overseeing and tracking the implementation of these measures, ASEH reviews and confirms the effectiveness of its human rights governance practices. It standardizes the outcomes of due diligence, the cases of human rights violations, and the effectiveness of improvements. Moreover, it establishes clear communication channels with stakeholders and publicly discloses relevant human rights management information. This ensures the continuous enhancement of its human rights management mechanisms, including but not limited to, reviewing and revising policies, regulations, procedures, as well as preventive and remedial actions in order to ensure the more effective execution of human rights protection efforts.

- **Formulate and continuously optimize human rights policies and due diligence mechanisms**
  Formulate and continuously optimize human rights policies and management frameworks with reference to UN human rights guidelines, the EU CSDDD, and the OECD Due Diligence Guidance for Responsible Business Conduct, while establishing human rights management organizations and due diligence processes.



- **Identify and assess adverse human rights and environmental impacts**
  Identify and asses salient human rights risks within own operations and value chain partnerships through questionnaires, data monitoring, or audits (e.g., RBA SAQ and RBA VAP).
- **Take mitigation and remediation measures**
  Establish improvement plans based on salient human rights risk issues to prevent, cease, or minimize actual and potential advers impacts on human rights and the environment, and implement appropriate mitigation and remediation measures.
- **Provide grievance channels and establish handling mechanisms**
  Establish grievance handling mechanisms and provide communication and feedback channels, ensuring that complainants are protected from retaliation or adverse treatment.
- **Communicate with stakeholders**
  Disclose human rights policies, standards, and relevant human rights managment information on the official corporate website.
- **Monitor and evaluate the effectiveness of measures**
  Continuously track and monitor the effectiveness of implemented mitigation and improvement measures through audits, and standardize the improvement outcomes.

Target	Impacted Parties	Human Rights Issues	Policy	Responsible	Due Diligence	Grievance Mechanisms and Communication Channels
Employee	Employees, Female Employees, Foreign Employees, Young Workers	Prohibition of Forced Labor, Working Hours, Wages and Benefits, Non-Discrimination/ Non-Harassment/Humane Treatment, Occupational Health, Safety and Hygiene, Emergency Preparedness, Young Workers, Data Privacy and Security	Human Rights Policy Statement Policy on the Protection of Privacy and Personal Data	Subsidiaries' "Employee Care and Development Taskforce"	• RBA SAQ and RBA VAP • Internal audits	1. **Internal whistle-blowing channels:** the internal whistle blowing channels of subsidiary companies 2. **External reporting channel:** Code of Conduct Compliance Reporting System https://coms.aseglobal.com/antifraud/ch.asp 3. **Personal Data Protection Inquiry and Communication Channels:** Hotline: +886-73617131 #83830 (Chief Administration Officer Office) Email: privacy@aseglobal.com
Joint ventures	Employees, Female Employees, Foreign Employees, Young Workers	Prohibition of Forced Labor, Working Hours, Wages and Benefits, Non-Discrimination/ Non-Harassment/Humane Treatment, Occupational Health, Safety and Hygiene, Emergency Preparedness, Young Workers			• Human Rights Issues Assessment Sheet	1. **Internal whistle-blowing channels**：the internal whistle blowing channels of supply chain partners 2. **External reporting channel**：Code of Conduct Compliance Reporting System https://coms.aseglobal.com/antifraud/ch.asp
Suppliers/ Contractors	Suppliers, Contractors, Young Workers	Prohibition of Forced Labor, Young Workers, Working Hours, Wages and Benefits, Occupational Health, Safety and Hygiene, Emergency Preparedness, Responsible Sourcing of Minerals, Anti-Corruption and Avoidance of Conflicts of Interest	Supplier Code of Conduct	Subsidiaries' "Supply Chain Management Taskforce"	• Supplier Sustainability Questionnaire • RBA SAQ • On-site Audit and RBA VAP	
Community	Community and Environment	Water Management, Noise, Air Pollution, Biodiversity, Climate Change Impact and Transition	Sustainable Development Best Practice Principles	Each facility	• Monitoring of Noise, Effluent, and Emission Sources at Facilities • TNFD Biodiversity and Nature Impact Assessment • TCFD Climate Risk and Opportunity Assessment	1. **Internal whistle-blowing channels:** the internal whistle blowing channels of subsidiary companies 2. **External reporting channel:** Code of Conduct Compliance Reporting System https://coms.aseglobal.com/antifraud/ch.asp
Customers	Customers, Suppliers, Contractors	Data Privacy and Security, Hazardous Substance Management	Policy on the Protection of Privacy and Personal Data, Cybersecurity Policy, Sustainable Raw Materials Policy, Environmental Responsibility Policy	Each facility	• Annual Risk Assessment • Internal Audit • Independent Third-Party Audit	

Human rights management standards and regulations:
1. Corporation Human Rights Policy Statement, please refer to https://www.aseglobal.com/en/pdf/human-rights-policy-en.pdf
2. Corporation Anti-Discrimination and Anti-Harassment Policy, please refer to https://www.aseglobal.com/en/pdf/anti-discrimination-and-anti-harassment-policy-en.pdf
3. Sustainable Development Best Practice Principles, please refer to https://media-aseholdco.todayir.com/20220324171126159296091_en.pdf
4. Code of Business Conduct and Ethics, please refer to https://media-aseholdco.todayir.com/20180622151727139618980_en.pdf
5. Supplier Code of Conduct, please refer to https://www.aseglobal.com/en/pdf/aseh-supplier-coc-en.pdf
6. Purchasing and Supply Chain Development Policy, please refer to https://www.aseglobal.com/en/pdf/2019_aseth_purchasingandsupplychaindevelopmentpolicy.pdf
7. Environmental Responsibility Policy, please refer to https://www.aseglobal.com/en/pdf/environmental-responsibility-policy-en.pdf
8. Policy on the Protection of Privacy and Personal Data, please refer to https://www.aseglobal.com/en/pdf/privacy-policy-en-2022.pdf
9. Sustainable Raw Materials Policy, please refer to https://www.aseglobal.com/en/pdf/sustainable-raw-materials-policy-en.pdf

Implementation and Outcome

Internal

The human rights risks of our manufacturing and business activities are mainly related to employee and local community interest groups. ASEH used the RBA Self-Assessment Questionnaire (SAQ) and Validated Audit Process (VAP) to perform risk management at our facilities worldwide. By examining the results of our human rights risk assessments of the past three years, ASEH was able to identify issues and interest groups that were vulnerable to human rights risks and prepare corresponding mitigation and compensation measures. According to the assessment results in 2025, potential human rights risk issues include working hours, non-discrimination/ non-harassment/humane treatment, occupational health, safety and hygiene, wages and benefits. Each year, ASEH has drawn up mitigation measures, which include raising human rights awareness via human rights training, ensuring sufficient manpower, management of working hours, improving occupational safety. For more information, please refer to Chapter 6.1 Talent Attraction and Retention and 6.3: Occupational Health and Safety of this report.

External

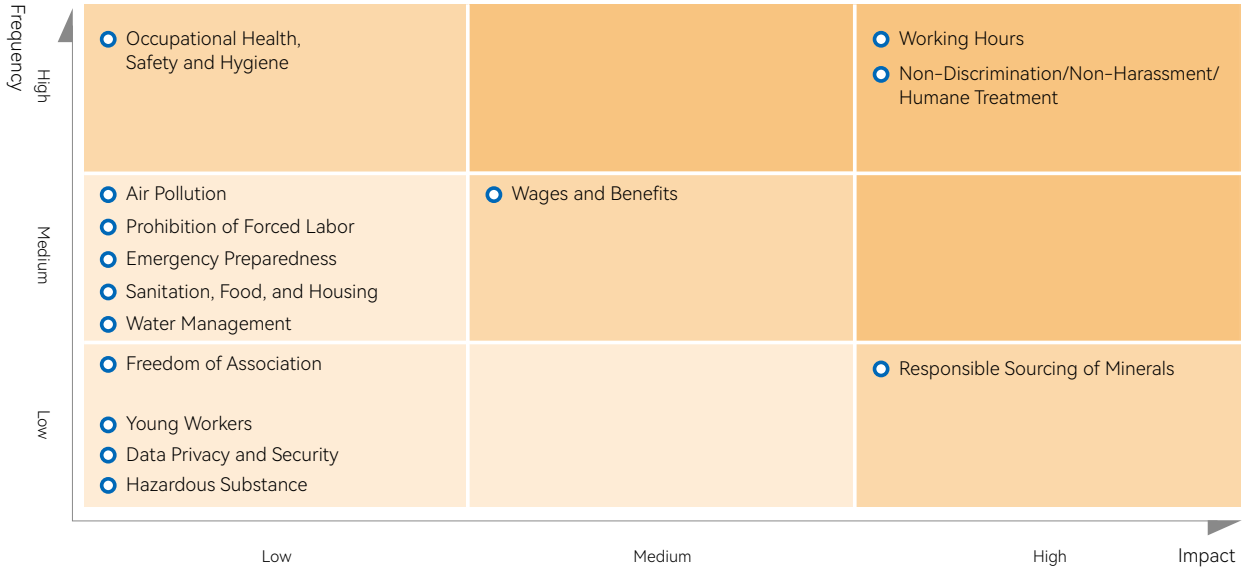
ASEH assessed human rights risks associated with the company's suppliers using supplier sustainability risk assessment questionnaires and the RBA SAQ. ASEH performed sustainability risk assessments on all tier-1 suppliers and conducted risk identification through the RBA VAP. Based on the assessment results in 2025, ASEH identified wages and benefits, occupational health, safety and hygiene, emergency preparedness and responsible sourcing of minerals as major human rights risks. ASEH then identified potential high-risk suppliers and adopted measures to verify and lower any risks. For more information, please refer to Chapter 7: Responsible Procurement of this report.

Human Rights Assessment

ASEH regularly evaluates potential human rights issues, including the following metrics: the proportion of issues assessed, the percentage of risks identified, and the rate of risk mitigation actions undertaken.

Target	A. % of total assessed in last three years	B. % of total assessed (column A) where risks have been identified	C. % of risk (column B) with mitigation actions taken
Own Operations and value chain partners	100	14.3	100
Suppliers/ Contractors	100	6	100
Joint Ventures	100	0	100

ASEH Human Rights Risk Matrix



Mitigation and Remediation Measures

The mitigation and remediation measures for the human rights risks identified with high frequency and high impact on companies in 2025 are as follows[1]:

Target	Salient Risk Issues		Mitigation Measures	Remediation Measures
Employees	Labor	• Working Hours • Non-Discrimination/ Non-Harassment/ Humane Treatment • Wages and benefits	【Systems】 ASEH complies with the legal and regulatory requirements of all operational locations and the approach is designed in support of the United Nations Universal Declaration of Human Rights (“UDHR”), the UN Global Compact (“UNGC”), the UN Guiding Principles on Business and Human Rights (“UNPBHR”), ILO Declaration on Fundamental Principles and Rights at Work(“ILO”), OECD Due Diligence Guidance for Responsible Business Conduct(“RBC”), Responsible Business Alliance Code of Conduct(“RBA”) and Corporate Sustainability Due Diligence Directive (“CSDDD”). ASEH is also committed to upholding local laws and regulations in the countries where ASEH operates, and reviewing the implementation of its human rights policies on a regular basis through membership on the RBA. • Non-Discrimination/Non-Harassment/Humane Treatment: ASEH has formulated the Anti-Discrimination and Anti-Harassment Policy to protect all ASEH employees from workplace discrimination and harassment. • Wages and benefits: Review compensation systems to ensure that wages, overtime pay, and other benefits comply with local minimum wage regulations and legal requirements, while considering whether they enable employees to maintain a reasonable standard of living (i.e., a living wage). Provide employees with accurate paystubs and establish payroll verification and internal audit systems to mitigate the risk of payroll errors. 【Education and Training】 • ASEH continuously conducts campaigns and training sessions on human rights issues, including human rights policies, non-discrimination/non-harassment/ humane treatment, to strengthen the internal awareness of human rights and implement the human rights protection activities wholeheartedly.	【Practices】 ASEH has established the human rights policy, committing to providing a workplace environment free from harassment, violence, discrimination, or inequality for all employees. • Working Hours: (a) Employment of sufficient manpower to meet manufacturing capacity and prevent manpower shortages and overtime. (b) Establishment of overtime management and tracking mechanism to prevent employees from working for seven or more consecutive days. (c) Develop an in-house working hours’ management and control system to help supervisors manage their subordinates’ working hours, send SMS or email alerts to employees working longer hours. 【Remediation】 • Non-Discrimination/Non-Harassment/Humane Treatment: Establish grievance and handling mechanisms to conduct post-incident reviews on root causes, as well as track, evaluate, and monitor individual cases. This ensures the effective implementation of disciplinary or corrective actions, prevents recurrence or retaliation, and guides continuous adjustments to workplace environments and systems. • Wages and benefits: Promptly issue back pay and make corrections upon discovering any underpayment of wages, overtime pay, or benefits. Conduct root cause analysis for major non-conformance cases, update management systems accordingly, and regularly track the implementation status of remediation measures. • When ASEH confronts other salient human rights issues, ASEH will negotiate and adopt measures based on internal procedures. 【Punishment】 • Non-Discrimination/Non-Harassment/Humane Treatment : For cases that constitute sexual harassment, the internal sexual harassment complaint processing committee shall issue a warning, disciplinary order, or another form of punishment to the offenders and require that they make an apology to the victims. Serious offenses may be grounds for dismissal. • When ASEH confronts other salient human rights issues, ASEH will negotiate and adopt measures based on internal procedures.

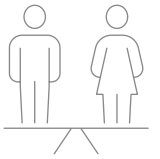
[1] The mitigation and remediation measures for other issues, please refer to the ASE Corporation Human Right Management Framework at https://www.aseglobal.com/en/pdf/human-rights-management-framework-en.pdf

Target	Salient Risk Issues		Mitigation Measures	Remediation Measures
Employees	Health and Safety	• Occupational Health, Safety and Hygiene	【Systems】 • All ASEH facilities worldwide have established OHS management organizations, and formulated methods and procedures that follow ISO 45001/OHSAS 18001 standards, the RBA Code of Conduct and local regulations. In addition to setting up a system for regular reviews, the OHS management system contributes effectively to preventing accidents. 【Education and Training】 • Occupational Health, Safety and Hygiene: (a) Public fire safety measures in accordance with the recommendations of the National Fire Protection Association; enhanced training in disaster preparedness and safety education. (b) Regular emergency evacuation drills for fire, earthquake, and composite disasters; review and improvement of warning and prevention measures. (c) In addition to the regular education and training, injury incidents and improvement of preventive measures are reviewed by ASEH each quarter.	【Practices】 • Occupational Health, Safety and Hygiene: ASEH facilities have established occupational accident and incident reporting and investigation procedures and management procedures. When an occupational injury incident occurs, the standard handling procedure is carried out and the incident is reported to the competent local authority according to management regulations and local laws and regulations. The injury incidents and improvement of preventive measures are reviewed simultaneously. ASEH facilities have established occupational accident and incident reporting and investigation procedures and management procedures. When an occupational injury incident occurs, the standard handling procedure is carried out and the incident is reported to the competent local authority according to management regulations and local laws and regulations. 【Remediation】 • Occupational Health, Safety and Hygiene: (a) ASEH identifies higher-risk operating environments within ASEH facilities such as locations that could expose employees to ionizing radiation, noise, dangerous chemicals and dust, and provide such employees with high quality protective equipment. (b) Health assessments performed by professional physicians in medical consultation to help employees with self-health management. • Assistance with medical insurance claims. • When ASEH confronts other salient human rights issues, ASEH will negotiate and adopt measures based on internal procedures. 【Punishment】 • ASEH will negotiate and adopt measures based on internal procedures.

Target	Salient Risk Issues		Mitigation Measures	Remediation Measures
Value chain partners (Joint Venture, Mergers)	Labor	• Wages and benefits • Non-Discrimination/ Non-Harassment/ Humane Treatment	【Systems】 • ASEH requests value chain partners to conduct annual audits or RBA VAP in order to mitigate risks. 【Education and Training】 • ASEH requests value chain partners to internally and externally promote the importance and implementation measures of human rights through regular education and training for reducing the human rights risks in advance.	【Practices】 • ASEH requests value chain partners to establish an internal sustainability audit system to carry out routine and ad hoc audits in order to continuously raise their sustainability. 【Remediation】 • ASEH requests value chain partners to adopt corrective measures for human rights risks and conduct follow-up on implementation. • ASEH requests value chain partners to provide guidance or financial compensation, or to implement policy changes or other compensatory measures for employees whose human rights have been violated. 【Punishment】 • ASEH requests value chain partners to terminate the relationship with their suppliers and request punitive liquidated damages when they are involved in salient human rights violation.
	Health and Safety	• Occupational Health, Safety and Hygiene		
Suppliers/ Contractors	Labor	• Wages and benefits	【Systems】 • Annual audits or RBA VAP to assess suppliers' human rights risks through company subsidiaries in order to mitigate risks. • Formulate ASEH conflict minerals policy and actively join as a member of the Responsible Minerals Initiative. Suppliers are required to comply with ASEH conflict minerals policy and actively assess and verify their supply chains. ASEH encourages suppliers to procure from non-conflict smelters recognized by the Responsible Minerals Assurance Process ("RMAP") or other equivalent independent third-party audit programs. • Establish a procurement raw material management process to conduct supplier surveys via the Conflict Minerals Reporting Template ("CMRT"). Suppliers are required to sign a letter of commitment to ensure compliance with ASEH conflict minerals policy and to guarantee accurate and full disclosure of their smelter sources. 【Education and Training】 • Through regular education and training, ASEH promotes the importance and implementation measures of human rights to suppliers for reducing the human rights risks in advance.	【Practices】 • ASEH has established a supplier sustainability audit system to carry out routine and ad hoc audits in order to continuously raise supplier chain's sustainability. 【Remediation】 • ASEH requests suppliers to propose and implement corrective measures for human rights risk issues and continuously track the progress of their improvements. • ASEH requests suppliers to provide guidance or financial compensation, or to implement policy changes or other compensatory measures for employees whose human rights have been violated. 【Punishment】 • ASEH shall terminate the relationship with suppliers and request punitive liquidated damages when suppliers are involved in salient human rights violation.
	Health and Safety	• Occupational Health, Safety and Hygiene • Emergency Preparedness		
	Ethics	• Responsible Sourcing of Minerals		







Protection of Privacy and Personal Data

Policies and Goals

ASEH values and cares about the importance of privacy and personal data protection. Accordingly, we have adopted a corporate policy on the protection of privacy and personal data and established relevant internal management measures; and requested our subsidiaries and their respective suppliers to collect, process, use, retain and disclose the personal data in compliance with the Personal Data Protection Act of Taiwan, EU General Data Protection Regulation (GDPR) and applicable laws and regulations on the protection of privacy and personal data in other countries or areas where they operate, ensuring the compliant operations and cooperating to protect the privacy and personal data and secure the rights and interests of data subject. Our corporate policy[1] sets forth clear guidelines and compliance requirement on the use and protection of personal data. We, our subsidiaries and their respective suppliers shall commit to collect, process, and use personal data to the extent not exceeding the necessary and minimal scope of specific purposes, and take appropriate and secure protection measures.

Advocacy and Implementation

To continue to enhance our employees' awareness of personal data protection compliance and ensure the compliance management and implementation, we regularly provide internal training course and important updates on relevant laws and regulations on the protection of personal data and compliance guidance. We also review the status of personal data security, assess any potential non-compliance risk our daily operations may be subject to and establish relevant management plans and measures in accordance with the results of assessment. Also, we complete RBA validated audit on bi-annual basis and the external RBA certified auditors carried out on-site audit of privacy aspects, among other management items, by reviewing our detailed internal management process related to (i) protect of personal data, (ii) safeguards to prevent unauthorized disclosure of personal data, (iii) monitoring procedures related to the protection of personal data, (iv) documentation and records with appropriate retention on-site/off-site and appropriate levels of access to ensure privacy conforming to regulatory record retention requirements. The latest RBA validated audit findings we receive rate "Conformance" for the foregoing privacy related aspects. In addition, we retained Ernst & Young, an independent third party accounting firm, to verify our compliance with Privacy Policy with respects to the matters on policy making, roles and responsibility, risk management, disciplinary actions, internal audit, public information, etc. The statement of above engagement provided by Ernst & Young is made available on our company website[2].

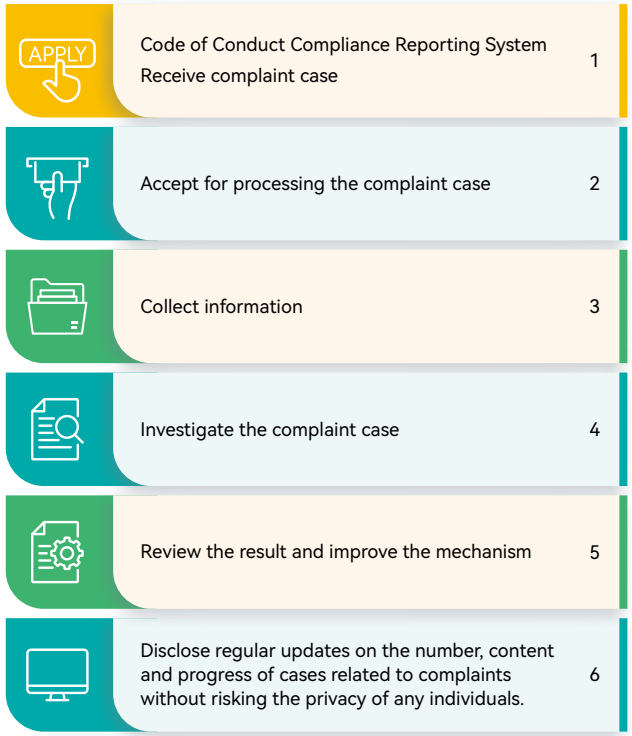
Use of Personal Data and Compliant

We have designated a department responsible for matters on the compliance with privacy and personal data protection and a hotline mechanism is also provided for our employees and external personnel to make inquiry or request about personal data based on his/her legal rights. We continue to monitor our use of personal data and throughout year 2025, we did not use collected personal data for any secondary purposes other than the specific purposes for which the personal data was first collected.

Our employees and external personnel may file complaint or report on the personal data matters via our reporting channels. Throughout year 2025, we did not receive any compliant or penalty related to personal data.

Type \ Source	Government Agency	Individuals or Other Type Parties
Compliant	none	none
Penalty	none	

Complaint Mechanism and Procedure



[1] Please refer to Policy on the Protection of Privacy and Personal Data at https://ase.aseglobal.com/privacy-policy/
[2] Please refer to the statement at https://www.aseglobal.com/en/pdf/coc-agree-upon-procedures-report-2026-en.pdf

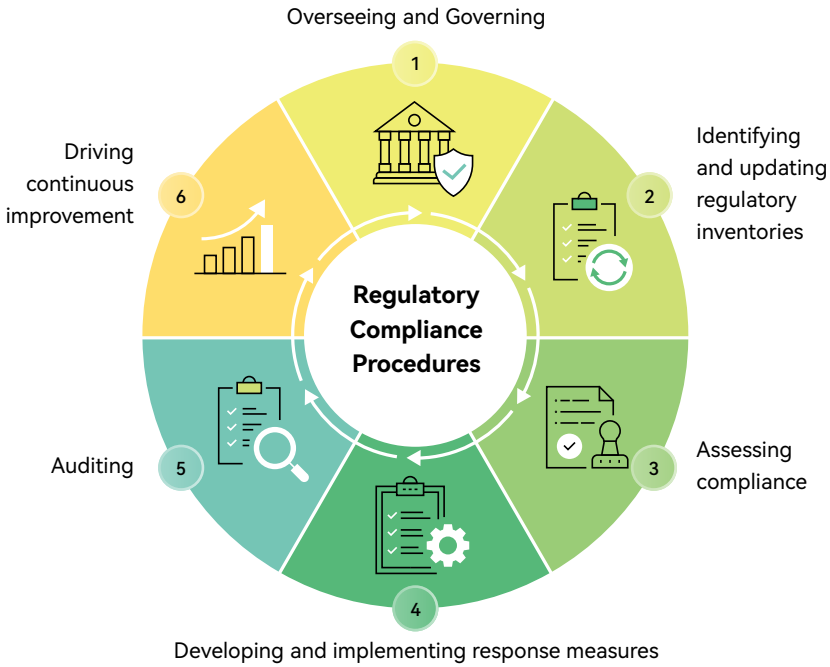
3.6 Regulatory Compliance

We conduct all our business activities in strict compliance with applicable laws and regulations. To ensure legal compliance, ASEH constantly maintains regular updates on domestic and foreign laws and policies that possess a potential impact on its operations and finances, and prioritizes regulatory compliance at all of its business locations. All subsidiaries shall comply with all applicable laws and regulations in the jurisdictions in which they operate.

The company's Corporate Governance Officer and Regulatory Compliance Department support board directors and the management team with overall regulatory compliance as well as supervise activities at our subsidiaries to ensure compliance with relevant laws and regulations. The company's regulatory compliance framework is implemented through six core processes: overseeing and governing, identifying and updating regulatory inventories, assessing compliance, developing and implementing response measures, auditing, and driving continuous improvement. These six pillars ensure the continuity and effectiveness of regulatory compliance. We have also optimized risk control mechanisms and management systems to assess and promptly mitigate any legal compliance risks across our operations. Accordingly, our subsidiaries are required to promptly report, via management systems, all incidences subject to corrective actions mandated by regulatory authorities or any penalties imposed. The responsible subsidiary shall also conduct a root cause analysis and implement corresponding improvement plans. Both the regulatory compliance department and audit department will verify and ensure the implementation of corrective actions, reporting the status to the board of directors annually.

In 2025, the company established a regulatory compliance management platform to continually strengthen compliance communication channels with all subsidiaries, while enhancing management mechanisms for integrating and identifying regulations, and monitoring and auditing compliance. The United States' Export Administration Regulations (EAR), Clean Competition Act (CCA), China's Anti-Unfair Competition Law, and the EU's General Data Protection Regulation (GDPR) are of particular significance to the technology sector, and are thus classified as our company's key compliance focus areas. The company also closely monitors the development of international sustainability and human rights legislation, including the EU's Corporate Sustainability Reporting Directive (CSRD), the European Sustainability Reporting Standards (ESRS), the Corporate Sustainability Due Diligence Directive (CSDDD), the Omnibus, the U.S. Uyghur Forced Labor Prevention Act (UFLPA), and the EU Artificial Intelligence Act (AI Act). In Taiwan, we focus primarily on the Taiwan Securities and Exchange Act, Labor Standards Act, the Employment Service Act, Occupational Safety and Health Act, Fire Services Act, Renewable Energy Development Act, Gender Equity in Employment Act, Sexual Harassment Prevention Act, the Regulations for the Management of Inventory Registration and Verification of Greenhouse Gas Emissions, the Renewable Resource Reuse Management Regulations, the Foreign Trade Act, the Personal Data Protection Act, the Cyber Security Management Act, and the Artificial Intelligence Basic Act, and other relevant regulations. As part of our regulatory compliance practices, we formulate or amend internal framework and enhance compliance awareness among board of directors, management, and employees of both the company and our subsidiaries through systematic training and announcements. This ensures that all personnel are well-informed and fully capable of adhering to relevant legal frameworks, thereby actualizing the core values of corporate compliance.

ASEH remains in resolute compliance with all major laws and regulations governing public listed companies in Taiwan, including the Company Act, Fair Trade Act, Securities and Exchange Act. In 2025, the company recorded thirty-two (32) cases that incurred financial penalties amounting to approximately US$65,153.52 imposed by authorities in the respective regions we operate. However, there were no incidents of significant fines (defined as a single penalty exceeding US$ 10,000) resulting from violations of regulations related to unfair competition, labor human rights, or environmental protection. In January 2026, we provided the board of directors with a status report for 2025, that included an overview of the corrective actions taken by the subsidiaries involved and an update on their regulatory compliance.

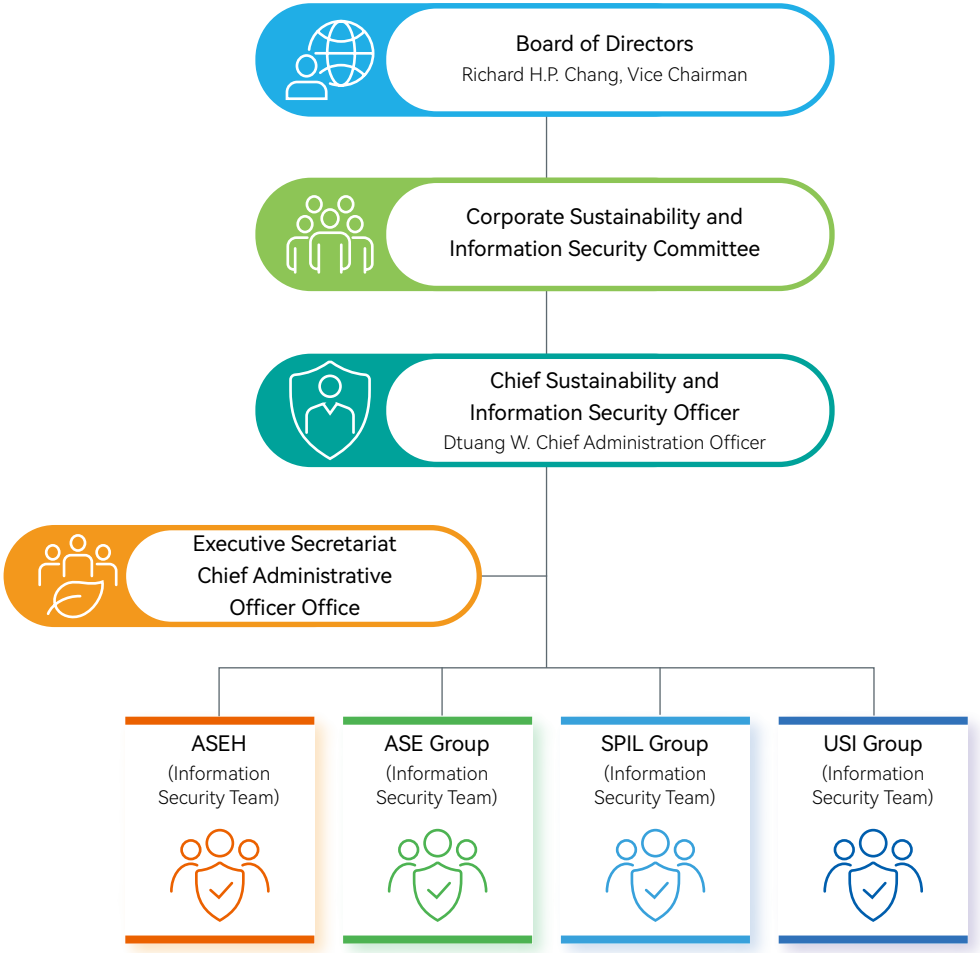


3.7 Information Security Management

Information Security Policy, Organization and Targets

To strengthen the company's resilience in information security (infosec) and respective management mechanisms, we have integrated an approach from the corporate governance perspective by putting in place a comprehensive set of infosec policy, conducting regular cybersecurity drills, and organizing employee education and training to enhance overall infosec awareness. The ASEH Information Security Policy[1] provides the highest level of management guidance to protect the confidentiality, integrity and availability of critical information assets, and to ensure compliance with relevant laws and regulations. With a robust infosec policy in place, ASEH is well positioned to boost customer trust, strengthen industry competitiveness, and maintain business continuity. We assess information security risks in accordance with regulatory requirements and business goals, and provide a status report to the senior management and the Board. The report offers a succinct overview of the infosec challenges and the current status, and forms the basis for the management and the Board to formulate additional guidelines, strategies and targets.

The Corporate Sustainability and Information Security Committee, comprised of board members, is chaired by Richard H.P. Chang, the current Vice Chairman of ASEH. The committee is responsible for overseeing the development of ASEH's overall information security strategy and maturity benchmarking, planning and supervision of enterprise-wide cybersecurity risk management, monitoring the implementation of information security operations across subsidiaries, and coordinating the integration of internal and external technical resources and threat intelligence. These efforts aim to strengthen ASEH's cybersecurity capabilities and reduce potential threats and risks. ASEH's Chief Information Security Officer (CISO), a position created by the Corporate Sustainability and Information Security Committee is concurrently held by the Chief Administrative Officer and Head of Corporate Governance, assumes responsibility for the establishment of the information security management framework that includes regular reviews with all subsidiaries of ASEH and implementing incident response plans. The committee provides a status report to the Board of Directors in the last quarter of each fiscal year. In addition, the Executive Secretariat of the Chief Administrative Officer Office is responsible for promoting and executing information security-related work, and each subsidiary establishes its information security team to be responsible for implementing information security operations. We regularly hold quarterly meetings of the Information Security Team to report and discuss the progress of our information security work, and invite external experts to share information security trends and significant issues.



[1] For more details on ASEH Information Security Policy, please refer to the link below: https://www.aseglobal.com/en/pdf/2025_ASETH_ISMP_EN.pdf

As our business continues to grow, the amount of information generated have also increased exponentially. Safeguarding the confidentiality, integrity and availability of information forms the cornerstone of ASEH's information security management. Besides identifying internal and external information security risks and formulating countermeasures, we regularly implemented the NIST CSF maturity assessment in all facilities every year. Our cybersecurity policies are formulated to ensure the highest level of network and system protection and mitigation of impacts from any disruption. At the same time, education and training are actively conducted to enhance employee awareness on the importance of information security and prevent major data breaches. Building resilience through a robust information security management system is key to corporate sustainability and will greatly boost stakeholder satisfaction.

Information Security Management Targets for 2035

1 Major Information Security Incidents : 0 cases

2 NIST CSF Maturity Assessment Coverage : 100%

3 Employee Information Security Education and Training Coverage : 100%

Artificial Intelligence Governance

Developments in artificial intelligence (AI) technologies are transforming the pace of digitalization in the workplace. While we are driving broad-based AI adoption and integrating the technologies across the company, we do recognize the need to prioritize AI governance. ASEH's AI governance is administered by the office of the Chief Administrative Officer, with responsibilities for coordinating with various company subsidiaries on the policy, framework and requirements. At the operating level, each department will integrate responsible AI practices relevant to their functions. We have published an 'Artificial Intelligence Management Policy[1] outlining AI governance principles and framework to guide AI adoption across the company. The policy covers the planning, development, deployment, use, monitoring and retirement throughout the AI adoption life cycle. It also outlines a structured approach to data privacy, information security, fairness, human feedback, transparency and interpretation, intellectual property, regulatory compliance, and ethical risk management. High-risk AI applications involving manipulation, exploitation of vulnerable groups, social scoring, and unauthorized biometric surveillance are explicitly prohibited.

To ensure the secure and responsible use of AI technologies, an AI tool as well as project application and approval process have been developed for our employees. Employees may only use authorized AI tools within the approved scope. AI applications involving personal data, confidential information, or other sensitive company data must comply with the classification and data protection policy, and undergo risk assessment and application reviews. Approved AI applications are continuously evaluated through model performance monitoring, model validation, drift analysis and AI risk assessments. Where necessary, models are adjusted or optimized to reduce the risks of bias, misuse or unintended outcomes. In addition, we have adopted the C.R.I.S.P.E prompting framework to standardize safe and effective AI use. Regular employee trainings are also scheduled to strengthen awareness of AI use, risks and governance.

At present, we are primarily using AI to support data analysis and improve operational efficiency, and not relying on it for autonomous decision-making. Human involvement will continue to play a key role in strategic decision-making as a safeguard to maintain human autonomy and accountability. AI technologies have been progressively adopted in areas including smart manufacturing, predictive maintenance, process optimization and generative AI applications. Key performance indicators such as reduction in work hours, productivity improvements, yield enhancement and other metrics are evaluated to determine the efficiency of AI adoption, while the results are used to drive continuous AI optimization. AI-related concerns have also been incorporated into the company's existing grievance, incident reporting and feedback mechanisms, enabling stakeholders to raise concerns or recommendations for review and appropriate follow-up. When procuring AI equipment and developing AI infrastructure, energy efficiency shall be a key evaluation criteria. In addition, AI will be applied to continuously optimize our manufacturing process, equipment operation and resource allocation, improving operational efficiency while supporting sustainability development.

[1] For more details on ASEH Artificial Intelligence Management Policy, please refer to the link below: https://www.aseglobal.com/ch/pdf/2026_ASEH_AIMP_CH.pdf

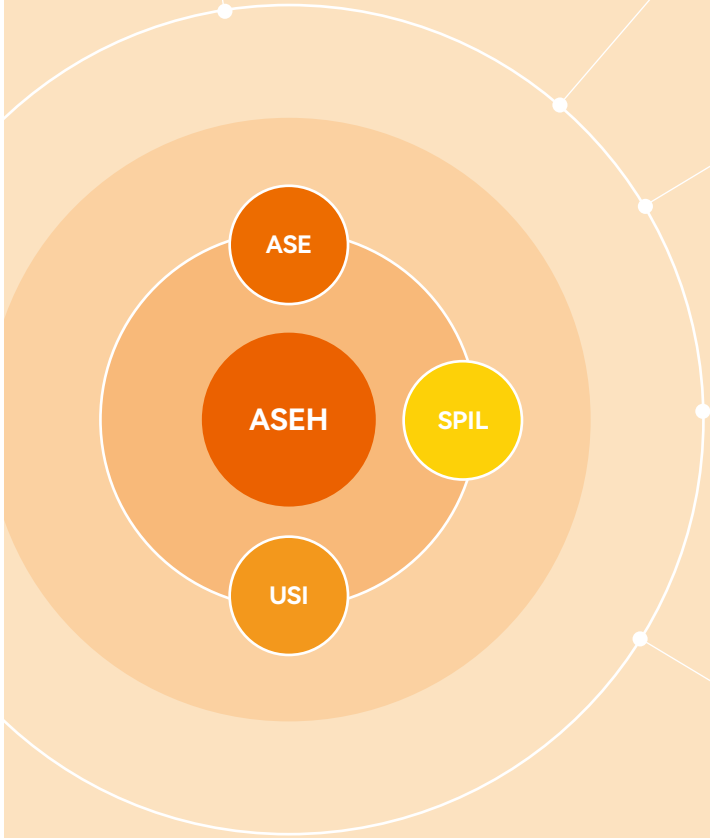
Information Security Implementation and Safeguards

Cybersecurity Maturity

We conduct comprehensive cybersecurity maturity assessments at all our subsidiary companies to ensure the resilience and effectiveness of their cybersecurity programs. We have engaged PricewaterhouseCoopers (PwC) to conduct maturity assessments for the IT and OA operations of our global subsidiaries based on the NIST Cybersecurity Framework (CSF) 2.0. The framework covers 6 core functions: Govern, Identify, Protect, Detect, Respond, and Recover. In 2025, the company's overall maturity level averaged 3.92, which is close to the Quantitatively Managed level of a structured, well-governed and mature cybersecurity management program.

Deloitte was engaged to conduct OT (operational technology) cybersecurity maturity assessments across our global manufacturing sites in accordance with the international standard IEC 62443. This encompasses a comprehensive evaluation of management practices and control systems for production and facility operations. Overall, our OT cybersecurity maturity is close to Level 3, demonstrating a well-established OT cybersecurity SOP and continuity in addressing security resilience of critical operational environments.

Cyber Resilience Collaborating Mechanism



Identify
- Cybersecurity policy formulation
- Cybersecurity organization estavlished
- Cybersecurity risk identication
- Classication and classication of cybersecurity incidents

Protect
- Cybersecurity training
- Social engineering rehearsal
- Cybersecurity information sharing
- Cybersecurity incident response rehearsal
- Supply chain cybersecurity management

Detect
- Cybersecurity assessment
- Cybersecurity maturity assessment
- Penetration testing
- Vulnerability scanning

Respond
- Cybersecurity incident investigation and analysis
- ASEH resource assistance
- Information disclosure and control
- Cybersecurity incident notication & response process
- Cybersecurity management system

Recover
- Cybersecurity incident review and improvement
- Stakeholder Communication
- Goodwill maintenance

Cybersecurity risk identification and management

We engage third-party audit firms annually to conduct information security audits, system vulnerability scans, and penetration testing to ensure that its information systems and network environments comply with security implementation standards. These efforts help enforce information security policies and customer privacy protection measures, effectively preventing the leakage of trade secrets and customer data. Tools used include Nessus for vulnerability scanning, BitSight for security ratings, the SecurityScorecard platform for analysis, and Red Team Assessments to evaluate system defense capabilities and incident response maturity. Additionally, the company provides monthly BitSight security rating reports to all sites for reference and continuous risk management improvement.

In addition to external audits, ASEH also conducts regular internal self-assessments of its Information Security Management System (ISMS) based on the NIST Cybersecurity Framework (CSF) and ISO 27001. These assessments evaluate the effectiveness of risk management, control measures, and incident response processes, and the results are reported to senior management and the Board of Directors. In the event of an unexpected cyberattack, the Information Security Management Task Force promptly convenes technical response meetings to analyze and review defense strategies, building a synchronized and comprehensive security network to respond to threats in real time.

Beyond managing operational risks from the perspective of corporate governance, we try to increase employees' cybersecurity awareness and enhance organizational operational capabilities as part of our focuses in cybersecurity management. All employees at ASEH must receive PIP cybersecurity educational training, including cybersecurity policy, cybersecurity management framework, cybersecurity control measures, etc. In 2025, a total of 153,679 individuals completed 110,890 hours of training courses. Additionally, occasional social engineering email drills were conducted to enhance employees' awareness of social engineering attacks through emails. Additionally, we will gradually introduce systematic management mechanisms to incorporate participation in cybersecurity meeting, educational training, incident management, confidential file labeling, antivirus/software security, and other cybersecurity-related projects in a systematic manner. Moreover, KPI monitoring and audits are conducted, extending the scope of management, and reaching every employee and every endpoint device. This will be integrated with employees' performance to reduce penalties and legal liabilities resulted from violations against cybersecurity regulations, as well as the impacts on business operations.

Increase cyber resilience

In 2025, no major information security incidents[1] occurred at the company. To strengthen our cybersecurity response and protection capabilities, the company established a well-defined set of "IT Security Incident Reporting and Emergency Response Procedures". The procedure serves as a unified employee guideline that outlines detailed specifications, including incident classification, response team structure, severity level determination, reporting and handling procedures, incident monitoring and closure, follow-up investigations, corrective actions, and evidence collection. Cybersecurity incident drills are also conducted regularly to enhance employees' awareness and improve response efficiency.

The ASEH Information Security Management System further integrates cyber threat intelligence sharing and incident reporting, two core functions that enable real-time monitoring of internal and external threats, ensure timely reporting and resolution of incidents, and significantly enhance overall risk visibility and collaborative defense capabilities. With the increase in cybersecurity threats and the risks they pose to business operations, we have adopted a risk-based approach by securing cyber insurance coverage for the company. This added layer of protection allows us to respond swiftly to incidences and contain the impact of any cyberattacks, minimizing potential losses to the company operations, customers, supply chain partners and facilitating rapid business recovery.

To ensure the sustainable operations of important businesses and prevent interruption of critical information systems as a result of material cybersecurity incidents, we conduct an incident recovery drill every six months which lays out the organizational structure diagram, scope, duration, critical information systems, participating units, participating personnel and their assigned tasks, backup personnel for the drill, implementation steps and processes of the drill, required resources, data recovery from backup, risk management during the drill, post-drill review and improvement processes, among others. The purpose is to ensure the company can leverage disaster response capabilities and disaster recovery mechanisms to quickly restore operations to a normal or acceptable level for the business, achieving the goal of uninterrupted operations of critical information systems. The drill will continue to be implemented to provide maintenance, management, and training to ensure the effectiveness of the backup systems.

[1] We define a major information security incident as any loss exceeding US$10 million

Cybersecurity Incident Reporting and Response Procedure

Cybersecurity Incident Detection 01
(Security Monitoring / Threat Intelligence Sharing / Employee Reporting)

Incident Analysis and Risk Assessment 02
(Incident Classification / Impact Assessment / Risk Categorization)

Notification and Incident Response Activation 03
(Cybersecurity Response Team / Cybersecurity Management / Management Team)

Incident Response and Cross-Functional Support 04
(Containment / Threat Mitigation / Cross-Department Coordination)

System Recovery and Business Continuity 05
(Service Restoration / Business Operations Continuity)

Post-Incident Review and Continuous Improvement 06
(Root Cause Analysis / Process Enhancement / Security Awareness and Training)

Information Security Information Exchange

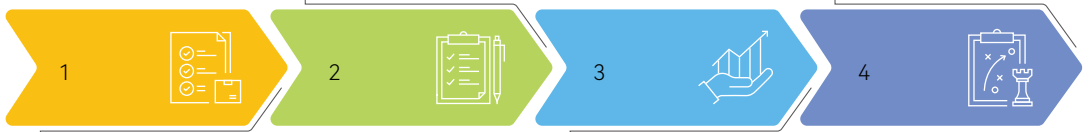
ASEH works closely with government agencies, local and international information security organizations including FIRST((Forum of Incident Response and Security Teams), Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC), and High-tech Information Security Alliance. As a member of the SEMI Semiconductor Cybersecurity Committee, we are actively driving the industry's adoption of SEMI E187 – Specification for Cybersecurity of Fab Equipment, a Taiwan-initiated security standard. Adopting the relevant infosec regulations, standards and industry intelligence allow us to integrate our internal management systems and expertise, to develop a comprehensive set of capabilities that will further strengthen our resilience.

At the same time, we are committed to meeting the expectations from our upstream and downstream supply chains and stakeholders on matters related to information security. ASEH's strong and robust security defense leads to a tightly-secured smart manufacturing environment and increases the company's competitive advantage as a sustainable enterprise.

Supply chain cybersecurity management

Digital transformation and the exponential growth of data exchanged between organizations are increasing cybersecurity risks in the supply chain. At ASEH, we are consistently strengthening cybersecurity resilience across our upstream and downstream supply chains through systematic cybersecurity assessments. Our key suppliers follow a four-stage management approach: current situation assessment, guidance for improvement, confirmation of outcome, and repeated monitoring. The process includes questionnaires, on-site assessments, document reviews and technical evaluations to enhance the maturity of suppliers' cybersecurity practices. Our deep focus in establishing a robust cybersecurity management framework has enabled the company to maintain a secure operation and resilient supply chain, while further enhancing the cybersecurity environment and standards of the semiconductor industry.

Procedures for supply chain cybersecurity assessment



Current situation assessment
Analysis of cybersecurity maturity assessment for daily operations and management

- Questionnaire survey
- On-site inspection

Guidance for improvement
Assist suppliers in optimizing management systems and implementing technical assessments

Results confirmation
Confirm that the current situation is better than before and subject to cyclic improvement mechanisms

- Written survey
- On-site inspection
- System management
- Technical survey

Cyclic survey
Regular or occasional survey

Information Security Certification and Information Security Measures Promote Results

Information security certification

ASEH prioritizes cybersecurity issues, identifying internal and external risks, and developing and promoting various key response strategies. It has earned recognition with international cybersecurity certifications, including ISO 27001, ISO 22301, ISO 15408, ISO 21434, IEC 62443, GSMA, and others. Through continuous management of corporate operations and adherence to international information security standards, ASEH rigorously reviews and optimizes cybersecurity workflows and management measures, enhancing operational resilience. This comprehensive approach safeguards smart manufacturing security and sustains competitive advantages for the company.

Information Security Investment and Results

ASEH approaches internal initiatives from a corporate governance perspective, establishing information security policies, conducting regular cybersecurity drills, providing cybersecurity education and awareness training for employees to enhance overall security awareness. It invites representatives from industry, government, and academia to share international cybersecurity developments regularly, increasing crisis responsiveness. Externally, ASEH actively participates in international cybersecurity organizations such as FIRST, TWCERT/CC Taiwan Cyber Security Alliance, and High-Tech Cyber Security Alliance. Through these communication channels, it shares the latest trends and action plans with industry peers and supply chain partners, elevating cybersecurity protection levels. Simultaneously, by aligning certification efforts with international standards, ASEH strives to mitigate cybersecurity threats, ensuring secure operations and fostering long-term, solid partnerships with customers and supply chain partners to provide more comprehensive and refined services.

International information security certification

ISO 27001	To build a stable and robust foundation for the IT environment, ASE Kaohsiung, ASE Chungli, Korea(Paju), SPIL, and USI Nantou continue to improve and implement cybersecurity risk management targeting critical information systems that are essential to the operation of crucial facilities.
ISO 22301	ASE Kaohsiung, ASE Chungli, SPIL and USI Nantou have successively obtained the BCMS (business continuity management system) ISO22301 certification to strengthen crisis management and disaster response.
ISO 15408	ASE Kaohsiung , ASE Chungli and ASE Singapore have been certified to EAL6, the highest level of security certification, creating a manufacturing environment and management system that comply with international standards for safe products and enhancing the safety management mechanisms for product transportation. We provide cybersecurity guarantees for manufacturing processes such as packaging and testing to offer better customer service.
ISO 21434	ASE Kaohsiung is the first semiconductor assembly and testing facility in the world to receive the ISO/SAE 21434 international automotive network security standard certification with 100% compliance by being certified by TUV NORD of Germany.
IEC 62443-2-1	ASE Kaohsiung passed the German TUV NORD's professional evaluation and obtained the IEC 62443-2-1 certification, becoming the very first company to receive the certification in the semiconductor industry in Taiwan.
GSMA	ASE Kaohsiung has passed the mobile communication security certification standard and obtained the GSMA certification. As a manufacturer, it completed a comprehensive audit of the production sites and processes to comply with the UICC production safety standard (GSMA SAS-UP)
TISAX	USI Nantou, USI Zhangjiang, USI Kunshan, USI Mexico, and AFG Suzhou have all obtained the TISAX certification (Trusted Information Security Assessment Exchange), a standardized information security assessment framework for the automotive industry that enables secure data exchange and mutual recognition of assessment results.

Information Security Investment and Results in 2025

Cybersecurity policies, organizations, and goals	• Established the Corporate Sustainability and Information Security Committee • Zero material cybersecurity incidents • Develop the Artificial Intelligence Management Policy • Formulated three cybersecurity goals for 2035 • Convened four ASEH Information Security team meetings
Information Security Implementation and Safeguards	• Implementation of one ASEH Information Security Management System • NIST CSF maturity assessment for 28 sites • OT cybersecurity maturity assessment for 28 sites • Conducted red team assessment at 5 sites • Provided monthly BitSight security rating reports • Conducted internal audits based on NIST CSF and ISO 27001 frameworks • Two cybersecurity incident drills • Providing cybersecurity educational training to 153,679 individuals • Accumulating 110,890 hours of cybersecurity educational training • Ongoing cybersecurity insurance coverage • Continue to Promote Supplier Cybersecurity Assessments
Cybersecurity certification	• ISO 27001 certified (ISMS): ASE Kaohsiung(TUV NORD), ASE Chungli(TUV NORD), Korea(Paju)(LRQA), SPIL(BSI), and USI Nantou(TNV) • ISO 22301 certified (BCMS): ASE Kaohsiung(BSI) , ASE Chungli(TUV NORD), SPIL(BSI) and USI Nantou(DQS) • ASE Kaohsiung certified with IEC 62443-2-1(TUV NORD) • ISO 15408 EAL6 highest-level certification: ASE Kaohsiung(BSI), ASE Chungli(ANSSI), and ASE Singapore(BSI) • Obtained TISAX (ENX) certification for the USI Nantou, Zhangjiang, Kunshan, Mexico, and AFG Suzhou sites