1 Sound Governance, Integrity-Based Management

Hon Hai Technology Group (Foxconn) upholds "Sound Governance, Integrity-Based Management" as its core strategy, continuously strengthening its board governance, integrity-based management, enterprise risk management, and information security and privacy protection mechanisms. Through an institutionalized oversight structure and transparent governance practices, the Group enhances corporate resilience and safeguards the rights and interests of shareholders and all stakeholders.

- **Board governance and participation maintained at a high level**: In 2025, the average attendance rate at Board of Directors meetings reached **100%**. The performance evaluations of the Board of Directors, Audit and Risk Committee, Remuneration Committee, and Nominating and Corporate Governance Committee averaged **4.99**, **4.99**, **4.96**, and **5.00** points, respectively, further strengthening the Board's oversight and decision-making effectiveness.
- **Board diversity and independence continued to improve**: The current Board comprises **33.33%** female directors and **55.56%** independent directors, both meeting the annual management targets, continuously optimizing the Board's diverse composition and independent oversight function.
- **Corporate governance performance recognized externally**: Foxconn ranked in the **top 20%** in the Taiwan Stock Exchange's 12th Corporate Governance Evaluation, reflecting the Group's continued efforts to refine its corporate governance mechanisms and information transparency.
- **Anti-corruption systems and integrity management continued to deepen**: In 2025, the recertification and renewal of the ISO 37001 Anti-Bribery Management System was successfully completed. Anti-corruption training coverage among Board members reached **100%**, with a total of **552,722** employees in Taiwan, mainland China, and Vietnam completing anti-corruption training, along with **1,033** suppliers completing the relevant courses.
- **Enterprise risk management mechanisms continued to be institutionalized**: In 2025, a total of **320** risk reviews were completed through structured questionnaires and an annual inventory mechanism, summarizing six major risk dimensions and establishing a 5×5 quantitative risk matrix and risk grading methodology. The Group publicly disclosed its risk assessment logic and grading criteria for the first time, continuously enhancing its capabilities in the forward-looking identification and management of material risks.
- **Risk culture and internal control audits continued to be strengthened**: In 2025, more than **10** risk management training sessions were successfully held, with over 1,000 total participants. At the same time, the Group's risk management processes and disclosures obtained ISO 37301 Compliance Management System certification, continuously strengthening risk governance and alignment with international standards.
- **Information security governance and protection capabilities continued to improve**: In 2025, the Group recorded no major information and communication security incidents. The Group has established a global 24/7 Security Operations Center (SOC) and deployed **100** information security professionals to advance global cybersecurity joint defense and AI-enabled protection. In addition, **980** internal and external information security-related audits were completed in 2025, and the Group maintained an "A" excellence rating in external cybersecurity exposure assessments.
- **Cybersecurity awareness and operational resilience management continued to deepen**: In 2025, a total of **320** business continuity drills and tests were completed for core systems, and **51** phishing email test drills were conducted. The completion rate for application security training among development engineers reached **100%**, continuously enhancing company-wide cybersecurity awareness and the operational resilience of critical systems.

Material Topics

Corporate Governance | Business Ethics | Risk and Crisis Management | Information Security and Privacy Protection

SDG Alignment

Management Goals

Material Topic	Management Indicator	2025 Goal	2025 Performance	Achievement Status	2030 Long-Term Goal
 Corporate Governance	Board Diversity	• Female directors account for **30%**.	• Female directors account for **33.33%**.	Exceeded	• Plan to establish a Board-level Sustainability Committee: **100%** of board members possess diverse, cross-disciplinary expertise to strengthen sustainability decision-making capabilities.
	Board Independence	• Establish the principle that more than half of directors do not concurrently serve as Foxconn employees or managers.	• Independent directors account for **55.56%**.	Exceeded	
	Board Effectiveness	• Raise the performance evaluation targets for the Board of Directors, the Audit Committee, the Remuneration Committee, and others to an average of **4.80**. • Conduct an external professional team's performance evaluation of the Board of Directors and functional committees once every three years.	• In 2025, the Group successfully completed its external performance evaluation. The performance evaluation scores of the Board of Directors, the Audit Committee, the Remuneration Committee, and others averaged **4.99**.	Exceeded	
	Tax Policy	• The Group publicly discloses its Group tax policy.	• The Group disclosed its Group tax policy in the Sustainability Report ahead of schedule and simultaneously updated it on its official website.	Achieved Ahead of Schedule	
 Business Ethics	Anti-Corruption	• Complete the recertification and renewal of the ISO 37001 Anti-Bribery Management System.	• The ISO 37001 recertification and renewal was successfully completed.	Achieved	• Achieve **100%** follow-up coverage of existing cases and comprehensive screening of new violation cases, upholding a zero-tolerance principle.
		• Use the Group app to announce corruption and legal/regulatory violations, as the number of publicly disclosed cases increases **10%** annually.	• In 2025, published **24 posts** via the Group app for compliance violation announcements and anti-corruption advocacy, up **33%** year-over-year.	Exceeded	
 Risk and Crisis Management	Enterprise Risk Culture Building	• Advance the establishment of the Group's risk management system, strengthen risk culture and training, promote company-wide risk awareness, and hold risk management seminars and training courses.	• Foxconn successfully held more than 10 risk management training sessions, with over 1,000 total participants.	Ongoing	• Achieve **100%** system-wide data integration and build the "Group Risk Intelligence Hub."
 Information Security and Privacy Protection	Information Security Management	• Conduct penetration testing of 10 key systems annually, ensuring no major information security incidents with low impact. • Continuously improve the ISO 27001 Information Security Management System and assist business units in establishing their information security frameworks.	• In 2025, there were **zero** major information and communication security incidents.	Achieved	• Achieve **100%** ISO 27001 certification coverage across the Group's critical sites.

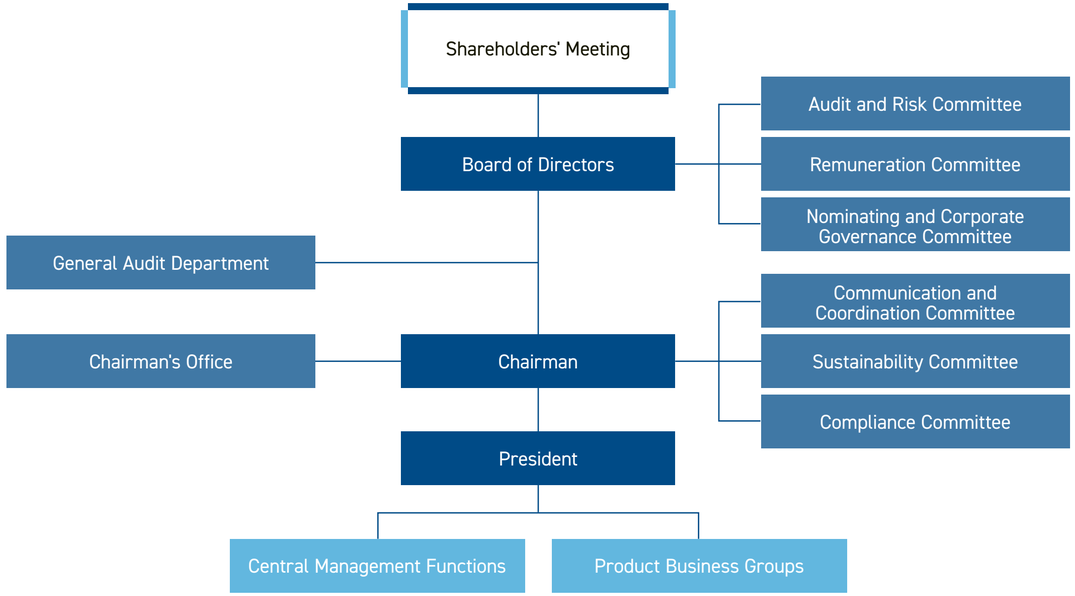
Corporate Governance

Foxconn Technology Group strictly complies with the Corporate Governance Best Practice Principles for TWSE/TPEx Listed Companies, continuously building a decision-making mechanism that balances sound governance with sustainable management—safeguarding shareholders' rights and interests while giving due consideration to the interests of all stakeholders. To fulfill its sustainability commitments, the Group continues to optimize its governance structure, linking senior executive compensation with sustainability performance and strengthening its sustainability management mechanisms. At the same time, the Group continues to enhance its enterprise risk management capabilities, proactively identifying and managing emerging risks, and strengthening customer privacy and data security management to maintain customer trust.

To further strengthen corporate sustainability and succession planning, Foxconn has designated the establishment of a sound succession mechanism as an important management priority, and officially launched its "Rotating CEO" program in April 2024, cultivating senior executives' holistic business perspective and management capabilities through a systematic rotation mechanism. Over the past year, the Rotating CEO has focused on the Group's operational integration, global campus coordination, management system optimization, and supply chain resilience enhancement, continuously advancing the linkage of central and local resources, management standardization, and digitalization, and supporting the Group's strategic development in response to geopolitical shifts and global deployment adjustments.

Board of Directors Structure and Operations

Group Governance Structure



Foxconn Technology Group has established a sound board governance structure comprising the "Audit and Risk Committee," the "Remuneration Committee," and the "Nominating and Corporate Governance Committee" to strengthen the Board's independence and oversight of its operations. The current Chairman, Liu Young-Way, is an executive director responsible for coordinating the Group's overall business direction and advancing major strategies.

The Company's Board of Directors currently comprises nine directors, including five independent directors, serving three-year terms and eligible for re-election. The Chairman is elected from among the directors. The Chairman represents the Company externally and oversees the Company's important affairs; the Company has also taken out liability insurance covering the scope of business execution of all directors.

Responsibilities and Members of the Board Committees

Committee Name	Core Responsibilities and Scope of Work	Board Members	Primary Collaborating / Executing Unit
Audit and Risk Committee	Oversees the fair presentation of the Company's financial statements, the effectiveness of the internal control system, and the status of regulatory compliance; and is responsible for overseeing the enterprise risk management (ERM) mechanism, precisely identifying and controlling mitigation measures for material risks including emerging risks and information security.	Independent Director Hwang Tsing-Yuan; Independent Director Wang Kuo-Cheng; Independent Director Liu Len-Yu; Independent Director Chen Yue-Min; Independent Director Hsu Tzu-Mei	Board Meeting Unit
Remuneration Committee	Formulates and regularly reviews the performance evaluation criteria and compensation policies for directors and senior executives, ensuring that the compensation system is deeply linked to the Company's long-term operational goals and sustainability (ESG) performance, in order to effectively motivate and retain core talent.	Independent Director Wang Kuo-Cheng; Independent Director Hwang Tsing-Yuan; Independent Director Chen Yue-Min	Board Meeting Unit
Nominating and Corporate Governance Committee	Formulates and reviews the corporate governance best practice principles, and identifies and nominates director candidates in accordance with the board diversity policy; is also responsible for planning senior executive succession programs (such as the "Rotating CEO" program) and overseeing the implementation of the Group's sustainability development strategy.	Independent Director Hwang Tsing-Yuan; Independent Director Wang Kuo-Cheng; Independent Director Liu Len-Yu	Board Meeting Unit

To ensure that directors have sufficient time and energy to fulfill their duties, the Company strictly complies with Taiwan's Regulations Governing the Appointment of Independent Directors and Compliance Matters for Public Companies, which stipulate that an independent director may not concurrently serve as an independent director of more than five other public companies (including listed, OTC, and emerging-market companies). Currently, all non-executive directors and independent directors of the Group strictly comply with the concurrent-position regulations, with none holding more than four director positions at other listed or OTC companies.

In addition to the concurrent-position regulations, the Company also reviews the qualifications of its independent directors to ensure the independence of its Board's decision-making. All independent directors must sign an independence declaration for the two years prior to their appointment and throughout their term, and must meet the following six core criteria:

- **No employment relationship**: Not an employee, manager, or director of the Company or its affiliated enterprises (except for those concurrently serving as independent directors within the Group in accordance with the law).
- **No significant shareholding**: The individual, their spouse, or minor children do not hold 1% or more of the Company's shares, and are not among the top ten shareholders.
- **No close kinship**: No kinship within the second degree of relatives with the Company's directors, senior executives, or major shareholders.
- **No business or financial conflict of interest**: No significant business dealings with the Company (such as receiving remuneration exceeding NT$500,000 for audit or consulting services in the past two years); and not a director or manager of the Company's major customers, suppliers, or shareholders holding 5% or more of its shares.
- **No controlling relationship**: Not a representative of a party that controls the Company's Board of Directors or holds a majority of its shares.
- **No disqualifying circumstances**: None of the negative qualifications listed in Article 30 of the Company Act (such as criminal offenses or bankruptcy), and not elected in the capacity of a government or corporate representative.

Building on the above governance foundation, Foxconn will continue to review its board composition and independent director configuration regularly, in accordance with regulatory requirements and the board diversity policy, and will continuously strengthen the Board's independent oversight and strategic guidance functions through sound governance mechanisms. For specific details on the Board's operations, please refer to page 22 of the Foxconn Group's 2025 Annual Report.

Board Diversity, Professionalism, and Effectiveness

Board Diversity and Professionalism

Foxconn Technology Group values the diversity and professionalism of its Board of Directors. In accordance with Article 20 of the Corporate Governance Best Practice Principles, the Group has formulated a Board diversity policy aligned with its operating model and long-term development needs. The selection of Board members takes full account of the following two core standards, so as to enhance the quality of decision-making and incorporate diverse perspectives:

- **Basic conditions and values**: Encompassing diverse aspects such as gender, age, nationality, and cultural background.
- **Professional knowledge and skills**: Possessing professional backgrounds in law, accounting, industry, finance, marketing, or technology, along with extensive professional skills and industry experience.

To ensure that the Board of Directors can effectively exercise its supervisory and governance functions, members must also possess the following eight core competencies: operational judgment, accounting and financial analysis, business management, crisis management, industry knowledge, an international market perspective, leadership, and decision-making.

The Group places great importance on the diverse composition of its Board and has set a specific management target for gender diversity, aiming for female directors to account for 30% or more, thereby strengthening the range of perspectives in Board decision-making.

Reflecting our commitment to diversity, the current Board of Directors comprises 55.56% independent directors and 33.33% female directors, with an average director tenure of 3 years—evidence of the continuous optimization of the Board's composition and structure.

Independent directors	Female directors	Average director tenure
55.56 %	33.33 %	3 years

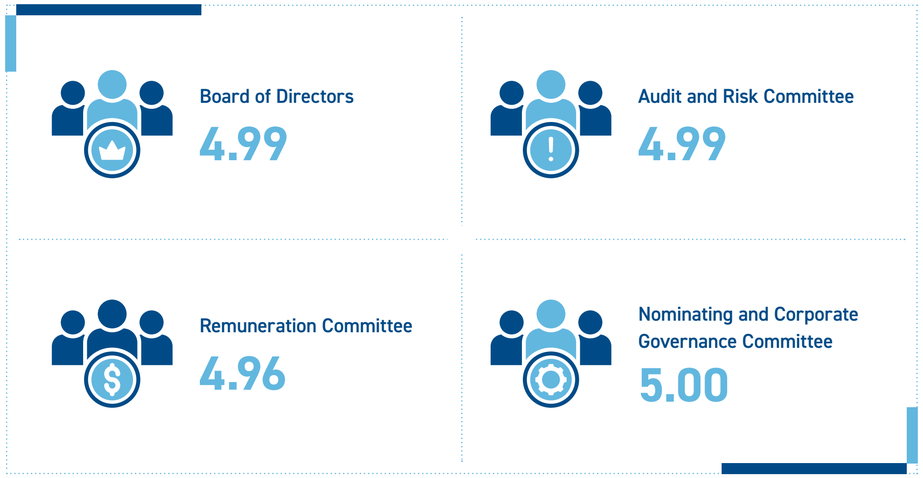
Board Member Information

Board Member	Title	Gender	Tenure (Years)	Professional Competencies and Industry Experience						
				Manufacturing	Brand & Channel	Finance & Investment	Technology & Research	Finance & Accounting	Marketing	Legal Practice
Liu Young-Way	Chairman	Male	6	✓	✓	✓	✓	✓	✓	
Chang Ching-Jui	Director	Male	0	✓			✓			
Chiang Shang-I	Director	Male	0	✓			✓			
Christina Yee-Ru Liu	Director	Female	5			✓		✓		
Wang Kuo-Cheng	Independent Director	Male	7		✓	✓		✓	✓	
Hwang Tsing-Yuan	Independent Director	Male	3			✓		✓		
Liu Len-Yu	Independent Director	Male	3			✓				✓
Chen Yue-Min	Independent Director	Female	3			✓		✓		
Hsu Tzu-Mei	Independent Director	Female	0			✓		✓		

Board Effectiveness and Performance Evaluation

In 2025, members of the Board of Directors actively fulfilled their duties, achieving an average meeting attendance rate of 100%. To safeguard shareholders' equity, the Group has expressly stipulated that any amendment to the Articles of Incorporation must be approved by resolution at the Shareholders' Meeting. In addition, the Group re-elects the Board of Directors every three years, ensuring that its composition consistently aligns with the Group's development needs and shareholders' expectations.

To continually enhance the Board's operational effectiveness, the Group implemented the Director and Committee Evaluation Method in November 2020. In accordance with this method, the Group conducts an internal performance evaluation annually and commissions an external evaluation by an independent professional institution or a team of experts and scholars at least once every three years. The evaluation results are finalized by the end of the first quarter of the following year. In 2025, the Group completed its self-evaluation through internal questionnaires, with the latest scores as follows:



In addition, Foxconn Group commissioned the Taiwan Business Integrity and Ethics Association to conduct the 2025 external performance evaluation of the Board of Directors. The association and its executing experts have no business dealings with the Group, ensuring full independence. The evaluation was conducted through questionnaire surveys and online video interviews, comprehensively assessing four major dimensions: the professional competencies of the Board of Directors, the Board's decision-making effectiveness, the Board's emphasis on and supervision of internal control, and the Board's attitude toward sustainable operations.

The evaluation results indicate a significant improvement in the effectiveness of the Group's decision-making information and communication. The Board's professional competencies and risk governance framework have continued to advance, and sustainability and talent issues have been elevated to the Board's strategic agenda. For specific evaluation results, recommendations, and the measures the Group plans to adopt, please refer to our official website: External Board Performance Evaluation - Foxconn Technology Group.

Board Conflict-of-Interest Recusal

To ensure the objectivity and fairness of decision-making, the Company has established strict conflict-of-interest recusal mechanisms in its Board Meeting Rules of Procedure and the Audit Committee Charter. Should a matter under discussion at a meeting involve the interests of a director or the corporate entity they represent, and pose a potential risk of harming the Company's interests, that director must proactively recuse themselves from the discussion and voting, and is strictly prohibited from exercising voting rights on behalf of other directors. In 2025, there were a total of 2 cases in which the Company's directors implemented recusal due to conflicts of interest (for detailed proposal information, please refer to the 2025 Foxconn Annual Report).

Board Sustainability Oversight and ESG Incentives

To ensure the effective implementation of our sustainability strategy, Foxconn Technology Group has established a top-down "Three-Tier Sustainability Governance Framework" with clearly defined roles and responsibilities (for the governance framework diagram, please refer to the Sustainable Governance and Management chapter). This framework drives the planning, execution, and oversight of sustainability issues:

Group Sustainability Governance Levels and Responsibilities

Governance Level	Person in Charge	Meeting Frequency	Specific Responsibilities and Scope of Oversight
Tier 1 Board of Directors Oversight	Chairman	At least quarterly	• Reviews the Group's key sustainability strategies, climate change response policies (e.g., Net Zero commitments), and medium- to long-term ESG goals. • Oversees the management team's ESG execution performance and resource allocation. • Ensures that the direction of sustainable development is closely aligned with the Group's overall business strategies and long-term interests.
Tier 2 Senior Management Oversight	Chairman of the Sustainability Committee	At least monthly	• Formulates specific ESG policies, short-, medium-, and long-term goals, and action blueprints. • Coordinates resources across business groups and manages material sustainability risks (including climate and cybersecurity risks). • Regularly assesses the achievement rates of ESG Key Performance Indicators (KPIs) and reports project progress and outcomes to the Board of Directors.
Tier 3 Execution Level	Sustainability Promotion Office	At least weekly	• Translates the ESG goals set by senior management into concrete action plans for the various campuses and business groups (e.g., energy-saving and carbon reduction projects, supply chain audits, and diversity and inclusion programs). • Manages sustainability data collection, inventory, and performance tracking as part of daily operations. • Compiles frontline execution status and challenges, reporting regularly to the higher-level committee.

2025 CEO Remuneration

Foxconn Technology Group links its compensation system with sustainability goals as an important mechanism for driving corporate transformation and strengthening management accountability. In 2025, the Company continued to optimize its CEO and senior management compensation policies, linking variable compensation to overall operational performance and long-term development goals. To fulfill its sustainability development commitments, we have further incorporated core ESG performance indicators into the annual performance evaluations of the CEO and senior executives, and adjust the payout ratio of variable compensation based on the achievement of the relevant goals, in order to enhance management's accountability for and execution of sustainability goals. For specific shareholding and compensation information, please refer to pages 18–19 of the Company's 2025 Annual Report.

To further enhance corporate governance and operational efficiency, and to ensure that business decisions are aligned with long-term value creation, the Company has established clear shareholding requirements for the CEO and members of the Executive Committee. In 2025, the CEO and other members of the Executive Committee held a percentage of Company shares commensurate with their positions and compensation, in accordance with internal regulations. This mechanism helps encourage the core management team to balance short-term operational results with long-term development goals, and further strengthens the alignment between management and shareholders' long-term interests, supporting the Company's steady and sustainable development.

In addition, Foxconn continues to maintain the fairness and information transparency of its internal compensation structure. In 2025, the Group continued to optimize its compensation management mechanisms, regularly reviewing employees' annual total compensation levels and conducting internal reasonableness assessments and benchmarking between the CEO's annual total compensation and the overall compensation level of all employees. By maintaining competitive and fair compensation distribution principles and a reasonable compensation multiple, the Group not only helps enhance the fairness of its internal compensation structure, but also enables stakeholders to more fully understand the Company's commitment to safeguarding employee well-being and implementing internal compensation fairness.

Financial Performance

The Group deeply understands that a sound financial structure is an important foundation for corporate sustainable development. In the face of external environmental changes such as the global economic situation, industry business cycles, and geopolitics, the Group continues to focus on long-term value creation, adopting a return on equity (ROE) of 12% and a return on capital exceeding 12% as its financial management direction. Through prudent operational strategies, capital allocation, and operational efficiency optimization, the Group strengthens its overall competitiveness and profitability, pursuing long-term stable growth in revenue and profit.

While pursuing long-term growth, the Group also emphasizes risk control and financial soundness, regularly conducting risk assessments to identify operational, financial, and market risks that may affect the Company's profit and loss, and formulating corresponding management measures accordingly. Adhering to prudent investment principles, the Group does not engage in high-risk or high-leverage investments, continuously strengthening its capital utilization discipline and financial risk tolerance to maintain operational resilience and safeguard shareholders' long-term interests. For the Group's specific 2025 financial data, please refer to the Foxconn Annual Report.

Tax Governance and Effective Tax Rate

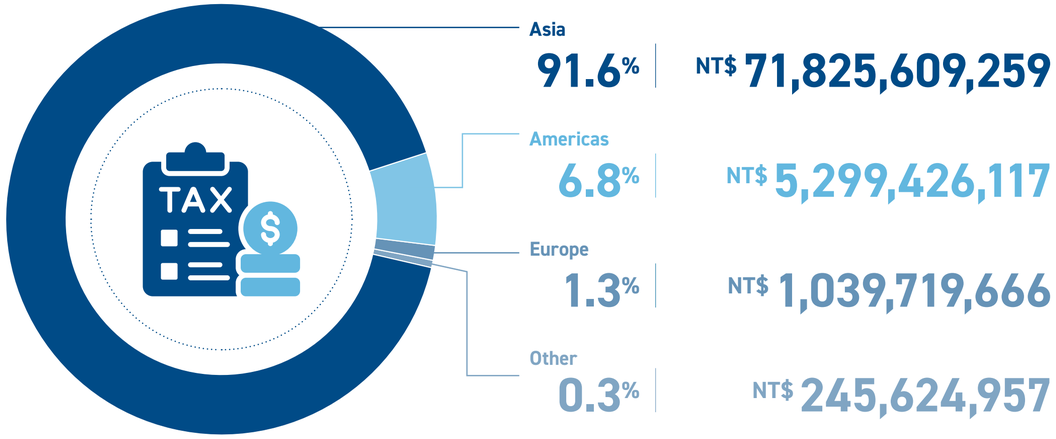
Foxconn Technology Group regards robust and transparent tax governance as a core part of fulfilling its sustainability commitments. By actively embracing our corporate citizenship responsibilities, we substantively drive shared economic prosperity in the global communities where we operate. To ensure tax compliance and risk control across our global footprint, the Group's Board of Directors serves as the highest decision-making and supervisory body for tax governance, responsible for approving the overall tax policy and overseeing the effective operation of tax management mechanisms. Accordingly, the Group officially promulgated the Tax Policy and Management Rules on August 10, 2022. This policy integrates tax governance with our vision for corporate innovation and transformation, establishing a governance framework that encompasses regulatory compliance, tax risk assessment, information disclosure, and tax management responsibilities. For detailed information on our tax policy, please refer to the official website link.

In terms of tax management practices, the Group strictly complies with the tax regulations of the jurisdictions where its operational sites are located and adheres to the management principle of "avoiding improper tax planning." For related-party transactions, we strictly adhere to the arm's-length principle and strive to maintain transparent, mutually trusting communication with tax authorities across regions, including participating in seminars held by tax authorities and external professional organizations to acquire new knowledge and exchange views. To strengthen risk control, when the Company and its subsidiaries file various tax returns, they implement tiered accountability and review-and-approval procedures in accordance with their respective duties, and properly retain relevant supporting documentation for review by the competent authorities. In addition, the Company addresses external investors' inquiries on tax issues through its central enterprise communication channel.

2025 Group Tax Information (Unit: NTD)

	FY2024	FY2025
Revenue	6,859,615,493,000	8,103,104,763,000
Pre-tax Profit (Loss)	211,875,157,000	293,444,866,000
Income Tax Expense (Current Year)	40,195,922,000	78,410,380,000
Effective Tax Rate (%)	18.97%	26.72%
Income Tax Paid	46,512,512,000	52,599,823,000
Cash Tax Rate (%)	21.95%	17.92%

Distribution of Income tax expense by the Group Across Global Tax Jurisdictions (NTD)



Business Ethics

Foxconn Technology Group regards integrity as an important principle of corporate governance, and has explicitly formulated its ***Code of Conduct for Integrity Management***, adopting a zero-tolerance stance toward any illegal or unethical conduct. The Group strictly complies with domestic and international anti-corruption and anti-bribery laws and regulations and, through comprehensive internal oversight mechanisms, ensures that all business activities conform to applicable laws and Company policies. To embed a culture of integrity throughout the organization, the Group arranges annual ethics and integrity training for employees, thereby strengthening their awareness of and compliance with integrity management practices.

Integrity Policy and Code of Conduct

Code of Conduct (CoC)

In terms of corporate conduct and responsibility standards, Foxconn upholds the principles of fair competition and integrity in its operations and has established legal compliance systems worldwide. As a member of the Responsible Business Alliance (RBA), the Group strictly complies with the RBA Code of Conduct and adheres to sustainability-related laws and regulations. Based on RBA standards, the Sustainability Committee established the Code of Conduct (CoC) in June 2008, which was subsequently updated in 2023. The CoC covers nine major areas: ethics, employees and human rights, health and safety, the environment, management systems, responsible mineral sourcing, anti-corruption, anti-slavery policies, and community engagement. In parallel, the Group formulated the Responsibility Standards to clearly define the CoC requirements and their implementation methods. All policies are reviewed and signed by senior management to ensure effective system execution and full compliance.

As international regulations and standards continue to evolve, the Group actively monitors these developments and plans corresponding adjustments. By the end of 2025, an internal assessment to update the Code of Conduct (CoC) and Responsibility Standards had been initiated. These updates are expected to benchmark against international standards such as RBA 8.0.2 and the EU Corporate Sustainability Due Diligence Directive (CSDDD), ensuring that the Group's operations consistently meet legal and compliance requirements. For the Group's Code of Conduct (CoC) and Responsibility Standards, please refer to the relevant links.

Anti-corruption Policy

All collaborations with suppliers, vendors, and clients must adhere to the Group's anti-corruption policy. Foxconn prioritizes corruption prevention in its management practices and strictly enforces its anti-corruption policy, which explicitly prohibits all forms of corruption, bribery, and improper conduct. The Group requires all employees to complete annual anti-corruption training to strengthen their compliance awareness and ethical judgment. Furthermore, all transactions with suppliers, business partners, and clients must comply with the Group's anti-corruption regulations.

In 2025, the Group identified 2 internal corruption incidents. The number of employees dismissed or subjected to disciplinary action for corrupt conduct was 2. There was 1 confirmed incident in which a contract with a business partner was terminated or not renewed due to corruption-related violations. On the legal front, 1 public legal case regarding corruption was brought against the organization or its employees during the reporting period, which resulted in 1 conviction.

2025 Internal Violation Incidents Report of Foxconn Group

Corruption or Bribery	Discrimination or Harassment	Customer Privacy Data	Conflicts of Interest	Money Laundering or Insider Trading
2	0	0	0	0

The Group has established a comprehensive anti-corruption training program encompassing online courses, in-person coaching, and dedicated supplier training, ensuring that relevant personnel across different levels and roles master anti-corruption knowledge and response capabilities. The course content covers domestic and international anti-corruption laws and regulations, company policies, case studies, risk identification, reporting procedures, and compliance management practices. Tiered training materials are designed specifically for senior executives, Board members, and general employees. The anti-corruption course is mandatory for all employees, aiming to deepen their understanding of ethical standards and policy requirements while reinforcing the Group's commitment to implementing integrity management across all levels of management and operations. Course completion status is also included as a criterion in employee promotion evaluations to further ensure the implementation of integrity-based operational requirements.

In 2025, employees in Taiwan, Mainland China, and Vietnam participated in online learning courses, with a total of 552,722 participants. The detailed statistics are summarized in the table below. In addition, the Group provides a Supplier Code of Conduct course that covers anti-corruption requirements; in 2025, a total of 1,033 suppliers completed this course.

2025 Foxconn Group Anti-corruption Training Coverage Rate

Number of Board Members Trained	Total Number of Board Members	Coverage Rate
9	9	100%

Note. Coverage rate calculation formula = Number of Board members trained in 2025 / Total number of Board members * 100%

2025 Foxconn Group Anti-corruption Training Employee Distribution

	Taiwan	Mainland China	Vietnam
IDL Employees (Including dispatched labor)	12,237	146,699	Not available
IDL Employees (Excluding dispatched labor)	12,193	146,699	Not available
DL Employees (Including dispatched labor)	2,156	289,633	Not available
DL Employees (Excluding dispatched labor)	1,460	229,409	Not available
Total Employees (Including dispatched labor)	14,393	436,332	101,997
Total Employees (Excluding dispatched labor)	13,653	376,108	Not available

Note. Data for Taiwan and mainland China reflect the status as of Wednesday, December 31, 2025, capturing the number of active employees within the Group who had completed the anti-corruption learning by that time; data for Vietnam reflect the status as of Thursday, October 30, 2025, capturing the number of employees who had completed the learning in Vietnam by that time.

Anti-competitive Policy

Through the Code of Conduct for Integrity Management, Foxconn explicitly regulates market competition, requiring all business activities to comply with applicable competition laws. The Group prohibits price-fixing, bid rigging, output or output quotas, and sharing or dividing markets by allocating customers, suppliers, operational territories, or lines of commerce. The Group also adheres to the principles of fair trade, ensuring that advertising content is truthful and responsible, thereby promoting healthy and orderly market competition. These regulations serve to safeguard consumer rights, enhance market transparency, and sustain an equitable competitive landscape.

In 2025, the Group continued to strictly implement the above regulations and was not involved in any improper conduct related to anti-competitive practices or antitrust violations. For specific policies, please refer to the link.

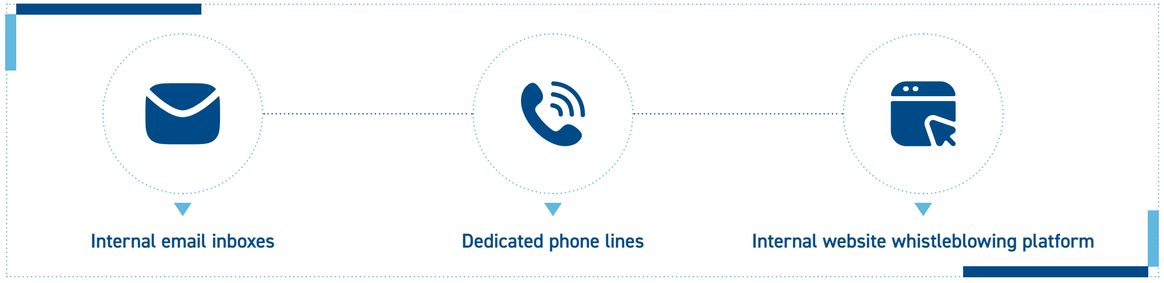
Integrity Management System and Whistleblowing Mechanism

Foxconn has incorporated anti-corruption issues into the scope of Board oversight, with management reporting on the related status to the Board of Directors at least once a year. The Sustainability Committee is responsible for formulating corporate social responsibility policies and management principles, with the Chairman, CEO, and heads of the various sub-committees jointly driving their implementation. Within the Group's Legal Department, a Fraud Prevention Division is responsible for establishing and maintaining the anti-fraud management system, while the Group's Audit Department conducts annual audits focused on key areas to ensure the continuous and effective operation of the anti-fraud and anti-corruption systems.

To further strengthen its whistleblowing and prevention mechanisms, the Group officially promulgated the Whistleblowing Procedures for Fraudulent Conduct in 2023. This standardized the processes for preventing, identifying, investigating, and reporting fraudulent behavior, with execution status reported regularly to the Board of Directors, the Audit and Risk Committee, or the General Manager. For the Group's Whistleblowing Procedures for Fraudulent Conduct, please refer to the relevant link.

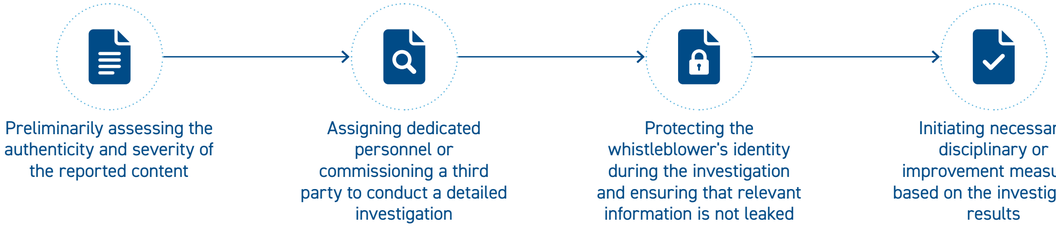
Integrity management and anti-corruption policies have also been integrated into employee performance appraisals and human resources policies, supported by a clear system of rewards and disciplinary measures. The Group explicitly stipulates and publicly discloses the disciplinary and grievance procedures for violations of integrity management regulations. Furthermore, it promptly discloses on its internal website the titles of violators, violation dates, details of the violations, and how the cases were handled (with personal privacy information redacted), providing transparent information on case processing. Foxconn obtained ISO 37001 Anti-Bribery Management System certification in 2022 and successfully completed its recertification and renewal in 2025, demonstrating the Group's commitment to and execution of continuous enhancements to its integrity governance system.

To strengthen early identification and effective handling, Foxconn has established multiple confidential whistleblowing channels, with a dedicated department centrally managing all reported cases. The whistleblowing channels are divided into internal and external routes, specifically including:



Whistleblowers may choose to submit reports anonymously or non-anonymously. All reported content is kept strictly confidential and accessible only to authorized personnel. Upon receiving a report, the dedicated department conducts an initial review, investigation, and handling in accordance with standard operating procedures. The investigation results and subsequent handling recommendations are then reported to the Board of Directors or the relevant supervisors.

The investigation process includes:



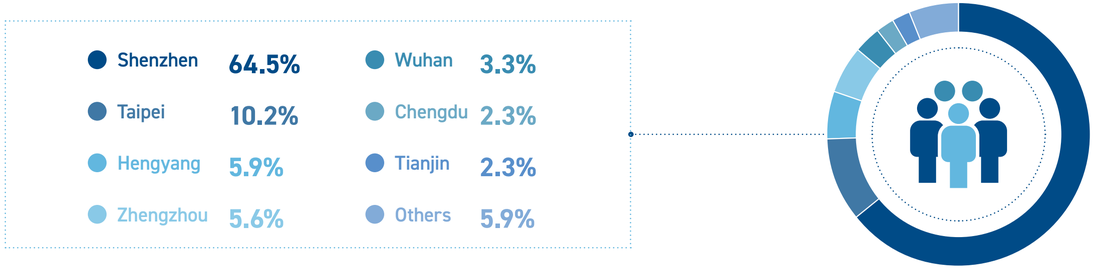
The Group explicitly prohibits retaliation against whistleblowers and provides training on using whistleblowing channels, helping employees and partners correctly understand the whistleblowing process and safeguarding whistleblowers' rights. All whistleblowing channels and related policies are publicly available on the Group's internal website, enabling employees and external stakeholders to access and use them at any time.

Internal Control and Audit

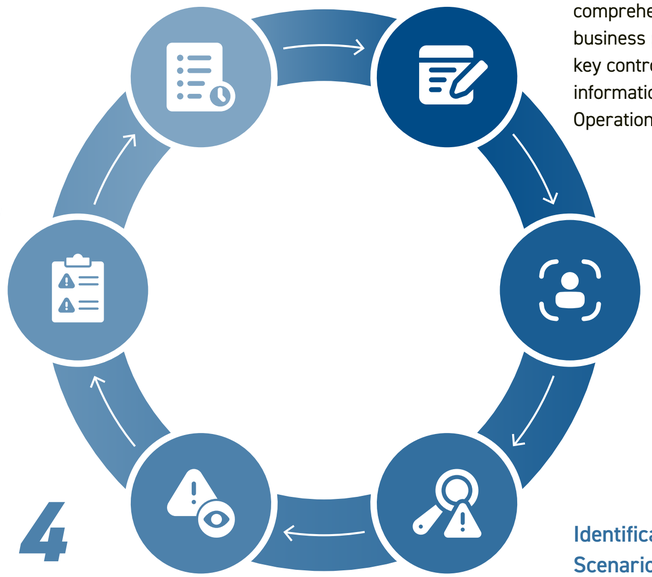
Foxconn Group places great emphasis on internal control and integrity risk management. Since 2022, the Group has fully complied with the ISO 37001 Anti-bribery Management Systems standard and regularly conducts corruption risk assessments. The core objective of internal control audits is to identify, assess, and manage the risks of corruption, bribery, and other improper behavior that may arise during the Group's operations. This ensures that all operational processes, organizational structures, and business partner management comply with internal control and regulatory requirements, further supporting integrity management and operational stability.

At the execution level, the Group completed comprehensive corruption risk assessments for 14 operational units in 2025, covering a total of 304 personnel. After careful evaluation, no material corruption-related risks were identified this year, indicating that the Group's internal control mechanisms are highly effective.

2025 ISO 37001 Distribution of Personnel by Job Function Risk Assessment



The internal control audit process primarily includes the following steps:



1 Departmental Operations Inventory
Each unit under evaluation conducts a comprehensive inventory of its departmental business processes, division of duties, and key control points, entering the relevant information into the "Departmental Operations Inventory Form."

2 Identification of Stakeholder Needs and Expectations
The needs and expectations regarding integrity management, compliance, and risk management of the internal and external stakeholders involved with the department are assessed and recorded in the operations inventory form.

3 Identification of Operational Risk Scenarios
For the identified operational items, scenarios that may involve corruption or bribery risks are analyzed. The identification results are entered into the "Operational Process Corruption and Bribery Risk and Control Assessment Form."

4 Review of Risk Control Measures
For the identified risk scenarios, the design and execution effectiveness of current control mechanisms are evaluated to confirm whether preventive measures are adequate. The results are recorded in the assessment form.

5 Residual Risk Assessment
The risks that may still exist after the implementation of existing controls (residual risks) are assessed and graded, serving as a basis for subsequent management optimization.

6 Continuous Improvement and Tracking
Based on the evaluation results, improvement recommendations are proposed, and relevant units track the execution to ensure the continuous optimization of internal control mechanisms.

The Group has also established internal control management mechanisms across its global subsidiaries. It supports all campuses and subsidiaries in conducting annual ethical audit self-assessments via an e-platform, covering system design, execution effectiveness, and key risk points, with reference to the standards of the internal control risk database. After each unit completes its self-assessment, the internal audit team conducts a review and consolidation, summarizing the assessment results and improvement measures, serving as an important reference for the Board of Directors and management to grasp the status of ethics governance implementation.

When internal auditors discover material violation incidents or determine that the Group faces a risk of severe damage, they must immediately prepare a detailed investigation report and notify the Board of Directors and the Audit Committee. This enables senior management to evaluate subsequent handling measures and improvement actions.

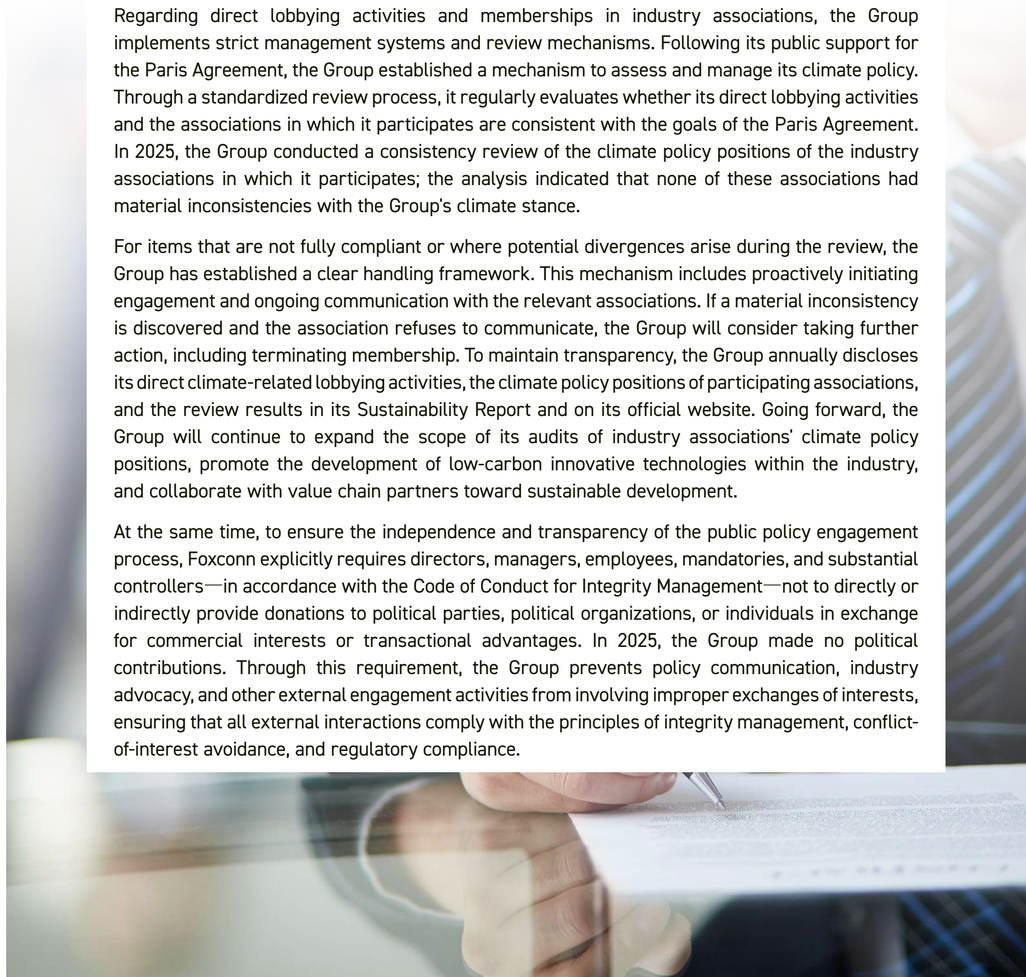
Policy Influence and Lobbying Transparency

Foxconn Technology Group explicitly states that its stance on climate change public policy is aligned with the Paris Agreement's goal of limiting global warming to 1.5°C. The scope of the Group's public policy engagement and climate advocacy encompasses all jurisdictions worldwide in which it operates. Within its governance framework, the Group has established clear regulations assigning the execution and oversight responsibilities for public policy engagement to the Public Relations Department. This department regularly reports to senior management to ensure that all external engagement activities comply with the Group's climate commitments and integrity principles.

Regarding direct lobbying activities and memberships in industry associations, the Group implements strict management systems and review mechanisms. Following its public support for the Paris Agreement, the Group established a mechanism to assess and manage its climate policy. Through a standardized review process, it regularly evaluates whether its direct lobbying activities and the associations in which it participates are consistent with the goals of the Paris Agreement. In 2025, the Group conducted a consistency review of the climate policy positions of the industry associations in which it participates; the analysis indicated that none of these associations had material inconsistencies with the Group's climate stance.

For items that are not fully compliant or where potential divergences arise during the review, the Group has established a clear handling framework. This mechanism includes proactively initiating engagement and ongoing communication with the relevant associations. If a material inconsistency is discovered and the association refuses to communicate, the Group will consider taking further action, including terminating membership. To maintain transparency, the Group annually discloses its direct climate-related lobbying activities, the climate policy positions of participating associations, and the review results in its Sustainability Report and on its official website. Going forward, the Group will continue to expand the scope of its audits of industry associations' climate policy positions, promote the development of low-carbon innovative technologies within the industry, and collaborate with value chain partners toward sustainable development.

At the same time, to ensure the independence and transparency of the public policy engagement process, Foxconn explicitly requires directors, managers, employees, mandatories, and substantial controllers—in accordance with the Code of Conduct for Integrity Management—not to directly or indirectly provide donations to political parties, political organizations, or individuals in exchange for commercial interests or transactional advantages. In 2025, the Group made no political contributions. Through this requirement, the Group prevents policy communication, industry advocacy, and other external engagement activities from involving improper exchanges of interests, ensuring that all external interactions comply with the principles of integrity management, conflict-of-interest avoidance, and regulatory compliance.



Risk and Crisis Management

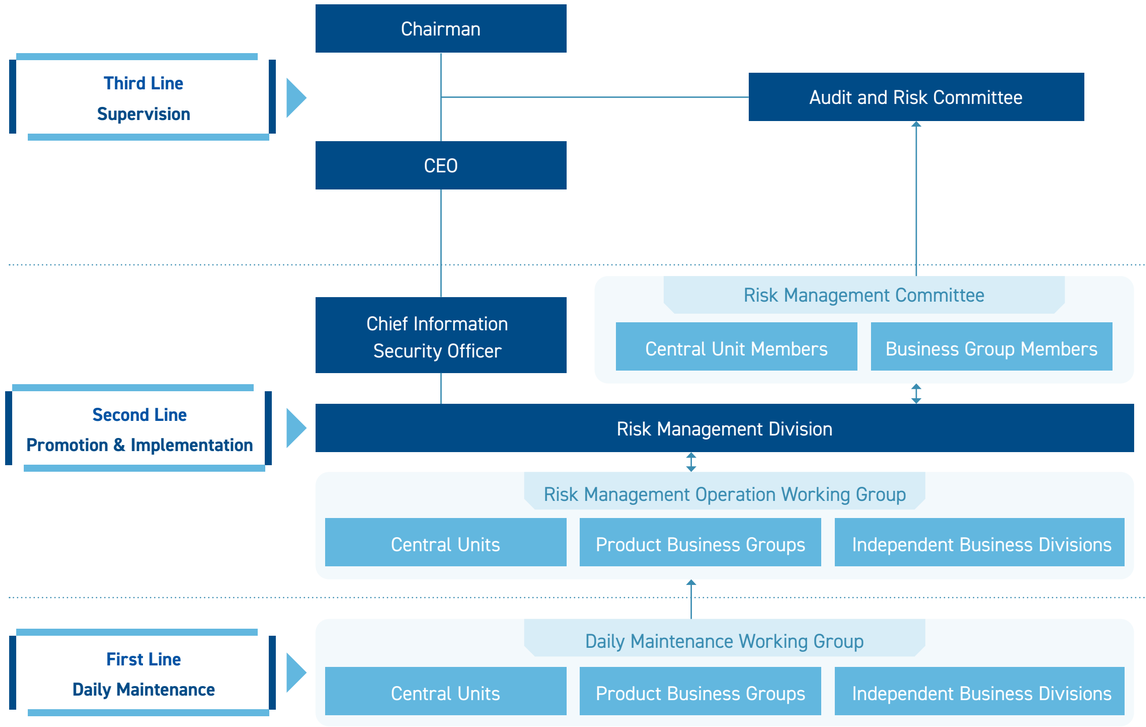
Foxconn Technology Group strictly complies with global regulations and deeply recognizes that effective enterprise risk management is essential for achieving corporate objectives, enhancing management efficiency, providing reliable risk information, supporting resource allocation, and ensuring the organization's long-term sustainability. To build a comprehensive risk management system and advance steadily toward the goal of sustainable corporate development, the Group formulated its Risk Management Policy with reference to the ISO 31000 and COSO ERM frameworks, as well as the relevant provisions of the Taiwan Stock Exchange's Risk Management Best Practice Principles for TWSE/TPEx Listed Companies, thereby establishing an effective operational mechanism for enterprise risk management.

Risk Governance Structure

As the highest governing body for risk management, the Foxconn Board of Directors focuses on regulatory compliance and the promotion and implementation of overall corporate risk management. By maintaining a clear understanding of the various risks encountered in operations, the Board oversees the effective functioning of risk management mechanisms and bears ultimate responsibility for the Group's risk management.

Group Risk Governance "Three Lines of Defense" Framework

With reference to relevant practices, Foxconn Technology Group continuously optimizes its risk management framework by establishing a corporate compliance and risk management system built on "Three Lines of Defense," which drives the effective operation of the overall risk governance mechanism:



Responsible for material risk control issues and for overseeing the coordination and operation of the overall risk mechanism. To assist the Board of Directors in supervising the effectiveness of the Group's risk management, the committee's core functions include:

- Reviewing risk management policies, procedures, and frameworks, and regularly reviewing their applicability and execution effectiveness.
- Approving the "risk appetite (risk tolerance)" to guide the appropriate allocation of Group resources.
- Ensuring the risk management mechanism can adequately respond to the risks faced by the Group and is integrated into daily operational processes.
- Approving risk control priorities and risk grading.
- Reviewing the execution status of risk management, proposing necessary improvement recommendations, and reporting to the Audit and Risk Committee regularly (at least once a year).

Serving as the second line of defense, this line is responsible for planning, executing, and supervising all material risk-related matters within the Group. It comprises three dedicated organizations that ensure the smooth advancement of risk management tasks:

- **Risk Management Steering Committee**: Responsible for overseeing risk management-related affairs and providing high-level guidance and resource support.
- **Risk Management Execution Team Representatives**: Dedicated to planning and executing various risk management tasks.
- **Central Risk Management Division**: Serving as the dedicated coordinating unit, it assists the risk management promotion and execution units, conducting cross-departmental risk coordination and management.

- Serving as the first line of defense, the relevant units are responsible for identifying, analyzing, and evaluating potential risks during frontline business execution. Through targeted risk management strategies and preventive measures, they effectively mitigate and control risk impacts and reduce the likelihood of risk events occurring.

Risk Management Process and Internal Audit

Risk Management

The execution of Foxconn's Enterprise Risk Management (ERM) mechanism strictly follows the five standard procedures of "risk identification, analysis, evaluation, response, and monitoring and review." In 2025, the Group's risk management team conducted a comprehensive risk inventory using structured questionnaires to assess the likelihood of occurrence, the degree of impact, and the effectiveness of existing control mechanisms for each type of risk.

Risk Identification

By consolidating the risk lists compiled by daily operational working groups and applying a systematic categorization based on Foxconn's industry characteristics, the Group has defined its potential risks across six major dimensions: strategic risks, operational risks (including information security), human resources risks, legal and compliance risks, financial risks, and emerging risks (including environmental sustainability, climate change, and infectious diseases).

After these risk assessment results were reviewed by the internal Risk Management Steering Committee and the Audit and Risk Committee, Foxconn formally defined its core risks for 2025 as Compliance Risks (e.g., international sanctions and tariff barriers) and Strategic Risks (e.g., geopolitical turbulence and overseas expansion challenges). At the same time, the Group maintains high-level monitoring and early-warning mechanisms for secondary risks, including market changes, human resource shortages, and exchange rate fluctuations. This ensures the timely activation of contingency measures, thereby reducing the Group's exposure to specific risks.

Risk Analysis and Evaluation

Upholding the philosophy of balancing risk control with operational returns, the risk management team works in tandem with the Group's strategic development goals to establish the annual risk appetite. Once approved by resolution of the Audit and Risk Committee and the Board of Directors, this metric is implemented across all business groups. The Group divides risk appetite into five levels to ensure that overall risk tolerance aligns with its operational strategies.

In terms of risk evaluation methodology, the Group uses a risk matrix to assess the probability of occurrence and the degree of impact for each risk event. Both dimensions are evaluated using a five-level quantitative scoring system, in which probability ranges from 1 (unlikely) to 5 (highest) and impact ranges from 1 (minor) to 5 (catastrophic). The risk management team calculates the risk score by multiplying the two levels; for example, if the impact is 5 (catastrophic) and the probability is 3 (medium), the risk score is 15.

Based on the scoring results, the Group classifies risk scores into five levels. Each level corresponds explicitly to a potential scale of financial loss and prescribes corresponding management measures. When a risk score exceeds 15, it is classified as a "Severe Risk." In such cases, the Group immediately convenes the responsible units for a special meeting to formulate specific response measures, which are incorporated into regular tracking and improvement plans. This ensures that critical risks remain within a controllable range, thereby further strengthening the robustness and resilience of corporate operations.

Group Risk Management Matrix

	1 Minor	2 Low	3 Moderate	4 Severe	5 Catastrophic
Very Likely 5	△Medium Risk	△Medium Risk	⚠Severe Risk	⚠Severe Risk	⚠Severe Risk
High 4	○Low Risk	△Medium Risk	△Medium Risk	⚠Severe Risk	⚠Severe Risk
Medium 3	○Low Risk	△Medium Risk	△Medium Risk	△Medium Risk	⚠Severe Risk
Low 2	○Low Risk	○Low Risk	△Medium Risk	△Medium Risk	△Medium Risk
Very Low 1	○Low Risk	○Low Risk	○Low Risk	○Low Risk	△Medium Risk

Risk Audit and Response

For the six key risks identified above, the Group has formulated corresponding risk mitigation and response measures, and manages and tracks them through systematic forms to ensure that all risk response measures are effectively implemented and closed out.

2025 Foxconn Group Mitigation Measures for Core Risks

Risk Type	Meeting Frequency	Risk Description	Mitigation and Response Measures
Compliance Risks	• 15 special meetings • 4 quarterly reports (presented to the Steering Committee and the Board of Directors)	**Sanctions and Tariffs:** Trade policies, export controls, and tariff barriers in major global markets are continuously shifting. Sanctions targeting the high-tech industry, in particular, may impact on the Group's cross-border transactions, supply chain stability, and operational costs.	We hold regular special meetings on trade compliance (typically monthly or postponed to the following month in the event of force majeure). These meetings provide immediate updates on international compliance cases and the latest regulatory developments. Cross-departmental teams—comprising IT, procurement, and business units—collaborate to develop a compliance review system. This system drives real-time, automated compliance screening for all order transaction regions and high-risk entities. Furthermore, we strengthen internal audits and risk early-warning mechanisms to mitigate the impact of sanctions and tariff fluctuations.
Strategic Risks		**Geopolitics and Overseas Expansion:** The unstable global political and economic landscape, geopolitical conflicts, trade wars, and policy shifts in emerging markets may lead to supply chain disruptions, operational hurdles, or increased uncertainty in overseas investments.	To address geopolitical conflicts and unpredictable policy risks, the Group continuously optimizes its overseas production footprint. Beyond China, we are actively expanding our manufacturing bases in regions such as Vietnam, the Czech Republic, Mexico, India, and the United States. This expansion strengthens the resilience of localized supply chains and mitigates the concentration risk of relying on a single region. During overseas expansion, our regional headquarters actively enhance communication and coordination with local governments. We also establish early-warning mechanisms for legal, political, and tax risks to ensure a consistently stable international operational footprint.

To ensure the effective execution of risk management and internal control processes, Foxconn Technology Group has established a multi-tiered, systematic internal and external audit and supervision mechanism. On a quarterly basis, the Group's Central Risk Management Division consolidates the risk inventory results from central units, product business groups, and independent business units, and then presents project progress reports to the Risk Management Steering Committee. The execution results of all risk identification, evaluation, and calibration efforts are reported to the Audit and Risk Committee and the Board of Directors at least once a year for project definition and effectiveness review. This ensures that the Group's risk management mechanism remains closely linked with high-level governance decision-making.

In terms of internal audits, the Group maintains an independent central audit unit responsible for the monthly review of various risk management activities and project progress, and it regularly reports identified issues and improvement recommendations to senior management and the Board of Directors. The internal control and audit process encompasses risk assessment and the formulation of annual audit plans, routine and special audits, e-platform self-assessments and reviews, audit conclusion reports, deficiency tracking, and the reporting of improvement results. This comprehensive process ensures that audit resources are prioritized on high-risk areas while strengthening the self-evaluation capabilities of all units.

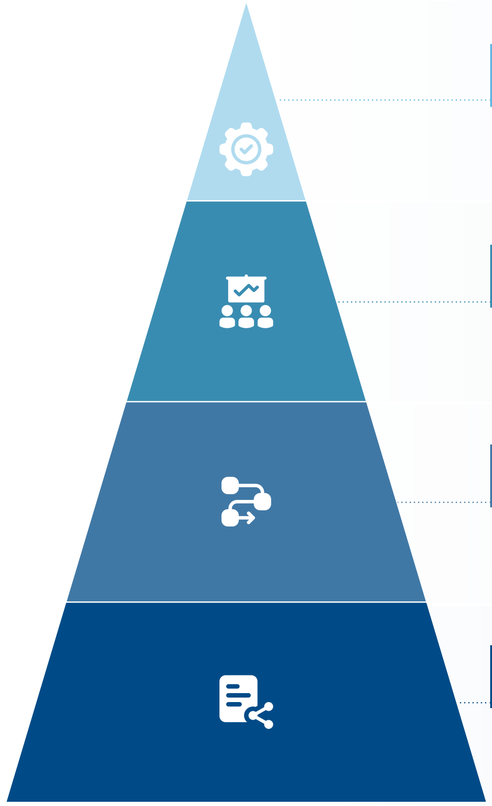
In terms of external audits, Foxconn continuously enhances the transparency and compliance of its risk management. In addition to internal audit checks, the Group's risk management processes and disclosures have obtained the ISO 37301 Compliance Management Systems certification. Each year, we commission international professional organizations (such as BSI) to conduct external verification of our management performance. Furthermore, quarterly meetings are held to track progress and promote relevant training, ensuring that our risk management system remains consistently aligned with international standards.

ISO 37301 Compliance Management Systems International Certification Issued by BSI in July 2025

For any internal control deficiencies and anomalies identified during the audit process, the audit unit continuously tracks their improvement progress. The results of these improvements are promptly reported back to the Board of Directors and the management team, serving as a critical basis for evaluating the overall effectiveness of the Group's internal control system. Through comprehensive internal and external audit mechanisms, together with regular reviews, Foxconn continuously strengthens the robustness and transparency of its risk management system, thereby ensuring the long-term stability of corporate operations and full compliance with regulatory requirements.

Risk Culture Building

Foxconn regards "company-wide risk awareness" as the key foundation for implementing its risk management mechanism and strives to embed a risk governance culture into the organization's DNA through top-down promotion. We integrate risk management into daily operations and organizational behavior through the following four practices:



Senior Governance Empowerment

The Group regularly provides dedicated risk management training for all non-executive directors and senior management. In 2025, we focused specifically on issues such as geopolitics in the high-tech industry, strategic export management, and global policy compliance. We hosted multiple specialized courses and leveraged our online learning platform to help the governance level stay abreast of international risk trends and management practices in real time.

Company-wide Awareness Training

In 2025, Foxconn held more than 10 risk management training sessions, with over 1,000 total participants, covering key topics such as global risks, policy compliance, geopolitics, and economic dynamics. Such training not only enhances employees' understanding of risk management principles but also strengthens frontline units' adaptability in the face of uncertainty.

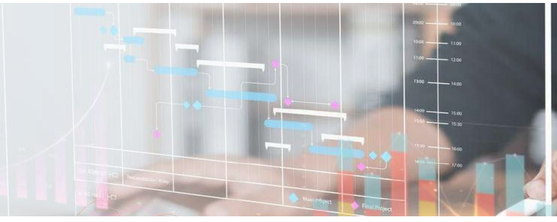
Business Process Integration

The Group actively incorporates risk management standards into its product and service development processes. Based on their business characteristics, each unit formulates and quantifies key risk indicators and thresholds, and conducts real-time monitoring using daily operational data, ensuring that all innovation development and operational decisions account for risk control.

Regional Political and Economic Information Sharing

The Group compiles monthly updates on regional risks and political-economic dynamics and distributes them as a reference for all central and business units. We also consolidate compliance cases and regulatory changes, conducting regular awareness campaigns that serve as reference materials for internal training across all units.

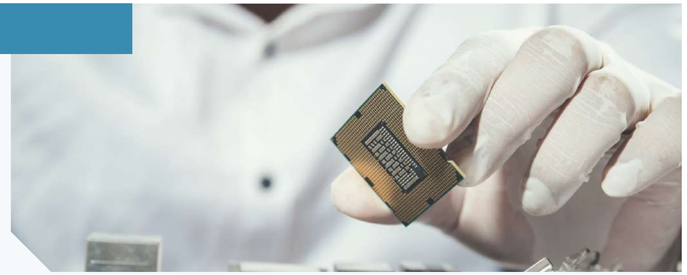
Looking ahead, Foxconn will continue to deepen its risk culture. By integrating risk management effectiveness into the performance appraisal and remuneration mechanisms for senior executives, we will further enhance the consistency between management decisions and the Group's long-term risk appetite. This approach will continuously strengthen our corporate operational resilience and sustainable governance capabilities.



Emerging Risk Identification and Mitigation

In the face of a rapidly changing global political, economic, and technological environment, Foxconn regularly identifies emerging risks that may have a material impact on the Group's operations over the next 3 to 5 years. By proactively planning response measures, we aim to enhance our operational resilience. The following are the top two emerging risks identified by the Group in 2025, along with their corresponding response strategies:

Emerging Risks 1



Rapid Iteration of Key Technologies and Supply Chain Resource Crowding Out Risk

Category: Technological, Economic

Description

As emerging applications like Generative AI drive a rapid surge in demand for computing power, the supply, demand, and cost structures of key components (such as High Bandwidth Memory [HBM] and advanced process chips) are becoming increasingly volatile. The industry faces supply chain imbalances and severe price fluctuations. With the accelerated pace of technological upgrades, an overconcentration of resources in a single technology will reduce the adaptability of production lines and create a resource crowding-out effect on traditional business segments.

Potential Impact

- The price fluctuation curve for key materials has deviated from traditional economic models. Furthermore, there are currently no precise metrics to evaluate the extent of long-term damage to the competitiveness of traditional businesses resulting from resources crowding out.

Mitigation Measures

- Diversified Supply Chain Strategy: Actively expand the diversity of suppliers and regional sourcing for key components to mitigate the risk of disruptions in any single supply chain.
- Dynamic Capital Allocation: Establish a cross-departmental capital allocation review mechanism to prevent the overconcentration of resources in a single technology or product line.
- Technological Flexibility Assessment: Regularly review the technological flexibility of production lines and alternative solutions to ensure the capacity to adjust swiftly during rapid market shifts.
- Key Material Price Early-Warning System: Introduce big data analytics and external industry intelligence to provide early warnings of abnormal price fluctuations in raw materials.

Emerging Risks 2

AI Applications and Global Digital Governance Challenges

Category: Social, Legal

Description

The rapid development of Generative AI technology has far outpaced current legal and ethical regulatory frameworks. While introducing AI can enhance corporate operational efficiency, it also introduces novel risks, such as blurred data privacy boundaries, algorithmic discrimination, and the generation of disinformation. If fabricated information produced by AI is maliciously exploited, it will cause incalculable and irreversible damage to corporate information security, reputation, and brand trust.

Potential Impact

- The resulting legal liabilities, reputational losses, and ethical lawsuits currently lack legal precedents, posing significant potential legal costs and governance challenges for corporate management.

Mitigation Measures

- AI Ethics Governance Framework: Establish a cross-departmental AI risk governance task force to formulate standards for AI transparency, explainability, and accountability.
- Dynamic Tracking of Regulations: Continuously monitor global trends in digital governance and AI regulations, proactively adjusting internal policies to comply with the latest legal requirements.
- Enhancement of Data Privacy and Security: Strengthen data classification, anonymization, and access control, while regularly conducting cybersecurity audits of AI systems.
- Employee and Supplier Training: Promote AI-related ethical and compliance training to elevate company-wide capabilities in identifying and responding to AI risks.
- Crisis Response Contingency Plans: Establish response procedures for AI misuse incidents, including real-time reporting, legal consultation, and mechanisms for brand reputation recovery.

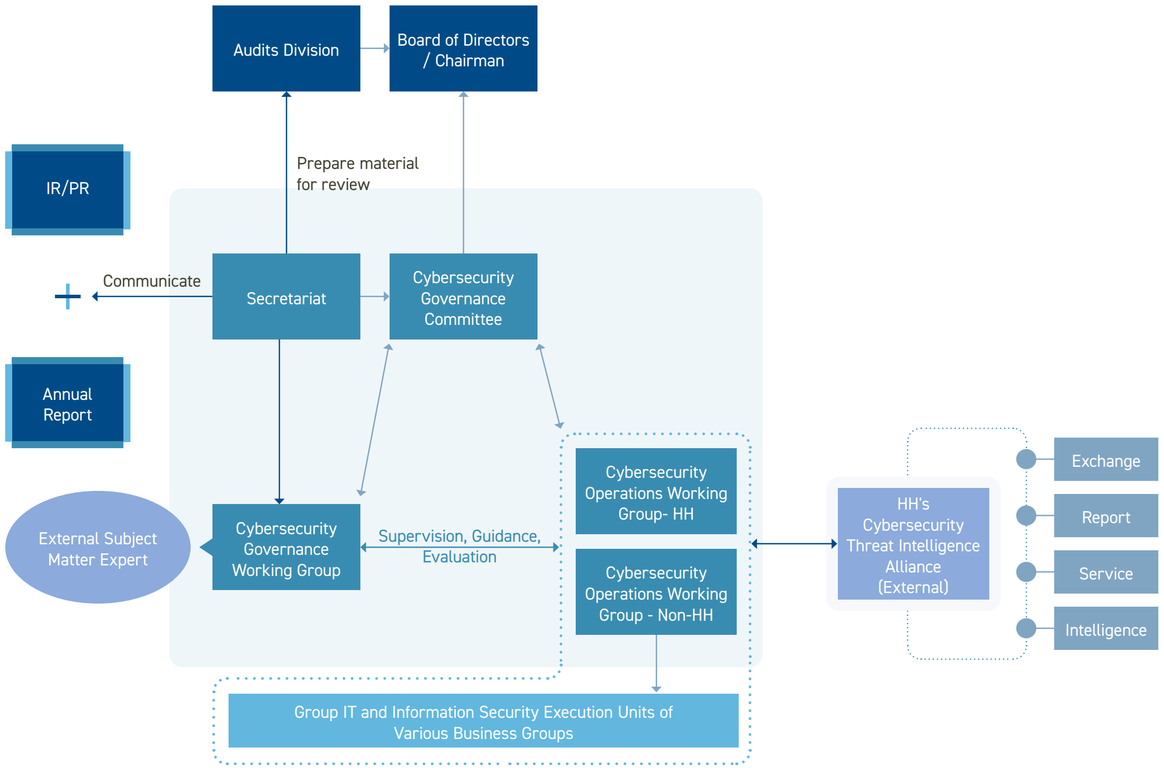
Information Security

Information Security Governance and Policy

Information Security Governance

Foxconn Technology Group regards information security as a critical management priority, essential for sustaining corporate operations and maintaining customer trust. Through systematic risk control mechanisms, the Group continuously safeguards the confidentiality, integrity, and availability of both operational and customer data. Information security management has been fully integrated into the Group's overall operational management and risk governance framework. In response to increasingly severe global cybersecurity threats, the Group has established an information security governance system that is overseen by the Board of Directors and driven by senior management, with regular reviews of related policies, resource allocation, and execution status.

Group Information Security Governance Framework



The Group has designated the Cybersecurity Governance Committee as the supervisory body for information security matters. The Committee's Secretariat regularly reports to the management team on information security governance planning, the Group's cybersecurity strategies, major risk defense guidelines, and resource allocation, thereby ensuring that the direction of information security development stays aligned with corporate operational goals.

To strengthen senior management's oversight and execution of cybersecurity issues, the Group established the Cybersecurity Governance Committee (hereinafter referred to as the Committee) as the highest-level organization for cybersecurity governance and decision-making. The Committee is chaired by the Board Chairman. Its core members include the Group Chief Information Security Officer (CISO), the Secretariat of the Cybersecurity Governance Committee, the Chief Information Officer (CIO), the Director of the Cybersecurity Research Institute at the Foxconn Research Institute, and the top executives of key subsidiaries (FII, FIH, FIT, FVT). Depending on the requirements of specific projects, the top executives of the Group's Finance, Risk Management, Human Resources, Legal, and Audit departments also attend meetings, ensuring that cybersecurity decisions are comprehensive and coordinated across departments.

Following a Board resolution, Dr. Wei-Bin Lee, CEO of the Foxconn Research Institute, was appointed as the Group CISO effective November 2022. In addition, the Cybersecurity Research Institute at the Foxconn Research Institute serves as the Committee's Secretariat. Leveraging the Cybersecurity Research Institute's research capabilities, the Group can promptly grasp international trends in information security governance, risk, and compliance. The CISO and CIO collaborate closely to jointly formulate high-level cybersecurity policies, oversee their implementation, and continuously refine the Group's information security governance and practices.

The Committee is responsible for coordinating the planning of the Group's information security governance structure, policy formulation, and culture promotion, and appointing the personnel responsible for each information security project. To ensure the effective implementation of policies, the Committee has two dedicated working groups under its purview:

- **Cybersecurity Governance Working Group**: Responsible for formulating information security governance strategies and guidelines, as well as developing information security policies and related regulations. This group also conducts regulatory compliance audits to ensure that the Group's operations meet global Information Security legal requirements.
- **Cybersecurity Operations Working Group**: Responsible for establishing and maintaining the Information Security architecture and protective equipment. This group carries out daily Information Security defense, threat monitoring, and risk assessment to ensure the effective operation of all cybersecurity defense mechanisms.

Information Security Policy

The Group continuously strengthens its information security governance to ensure the effective operation and ongoing optimization of its cybersecurity management system. The key focus areas of the information security policy in 2025 are as follows:

Enhancing Information Security Governance and Senior Oversight

Based on the organizational charter of the Cybersecurity Governance Committee (CGC), we clearly define the Committee's responsibilities and operating guidelines. The Committee convenes quarterly to review the Group's information security policies, standards, and mechanisms, and to stay abreast of information security trends and risk issues, thereby elevating senior executives' cybersecurity awareness and response capabilities.

Implementing Consistent Cybersecurity Audits and Internal Controls

In accordance with the ISO/IEC 27001 standard, we conduct annual on-site audits focusing on key control items to enhance the compliance and internal control capabilities of all business groups. Unscheduled document spot checks are conducted after each audit to ensure consistency among documentation, processes, and actual execution.

Refining Incident Grading, Reporting, and Response Mechanisms

With reference to NIST standards and relevant Taiwanese regulations, we have established principles for grading and reporting information security incidents and formulated response guidelines for ransomware events. This clearly delineates roles and responsibilities while strengthening cross-departmental collaboration. In 2025, the Group's Cybersecurity Research Institute conducted 2 educational training sessions and 3 drills to enhance familiarity with incident handling and improve response efficiency.

Elevating Defense Resilience and Resource Allocation Efficiency

We adopted the Open Web Application Security Project (OWASP) Cyber Defense Matrix (CDM) framework to build a visualized defense map. This strengthens our defense measures and resource allocation, thereby enhancing the efficiency of cybersecurity investments and our overall defense resilience.

Strengthening Vulnerability Management and Operational Impact Assessment

We established procedures for investigating and patching IT vulnerabilities, ensuring that technical weaknesses are identified, tracked, and controlled in real time. At the same time, we formulated guidelines for estimating financial losses from information security incidents, helping all units understand the operational impact of these events and optimize decision-making.

Expanding Joint Defense Collaboration

The Group established regional joint cybersecurity defense organizations and holds regular joint defense meetings to deepen internal collaboration and reporting mechanisms. Externally, we continuously maintain our partnerships with TWCERT/CC and the Taiwan Chief Information Security Officer Alliance to stay abreast of threat intelligence. Additionally, a 24/7 cross-timezone joint defense program is being planned to build a round-the-clock cybersecurity monitoring and management system.

Foxconn Technology Group continuously enhances its information security management. It extends the scope of cybersecurity protection across its entire supply chain, encompassing both internal operational environments and the management of external business partners. In addition to its existing systems, the Group continuously adjusts its management focus through regular reviews, internal self-assessments, and cross-unit collaboration, concentrating on the following five major dimensions:

2025 Group Information Security Management Focus Areas

Information Security Governance and Continuous Improvement

- Convenes the Cybersecurity Governance Committeequarterly, with senior management reviewing cybersecurity policies, documentation, and management mechanisms.
- Reviews cross-unit implementation status to ensure consistency with the Group's security principles.
- Tracks cybersecurity trends, regulatory requirements, and major risks to proactively plan response measures.
- Promotes the "Group Information Security Self-Assessment Form" and the annual Group cybersecurity audit to regularly review protection gaps, improvement progress, and the division of responsibilities.
- Continuously plans for cybersecurity insurance to mitigate the financial impact of operational disruptions.
- Implements the Open Web Application Security Project (OWASP) Cyber Defense Matrix (CDM) framework to effectively review the rationality of cybersecurity resource input and allocation, constructing a visualized defense map for the Group in 2025.

Data Integrity and Privacy Protection

- Implements next-generation secure remote access mechanisms to strengthen data security in remote work environments.
- Conducts data labeling management based on confidentiality classification.
- Utilizes encryption technologies, access controls, and platform audit trails to enhance data traceability.
- Deploys email anti-virus and anti-spam mechanisms.
- Dynamically adjusts defense strategies based on the latest malicious email attack methods.

Cybersecurity Threat Monitoring and Incident Response

- Establishes a dual-track cybersecurity defense framework of "proactive monitoring" and "rapid response."
- Monitors malicious actor dynamics and leakage risks in real-time through dark web threat intelligence platforms.
- Implements managed detection and response (MDR) systems for 24/7 monitoring of endpoints and network environments, instantly isolating abnormal assets.
- Establishes Emergency Response Committee (ERC) teams in all business units and executes regular drills.
- Activates the ERC mechanism for major incidents, executing detection, isolation, tracing, recovery, and post-incident retrospective analysis.

Employee Cybersecurity Responsibility and Awareness Enhancement

- Explicitly assigns personal information security responsibilities to all employees, requiring compliance with cybersecurity regulations in daily business operations.
- Integrates cybersecurity compliance into the employee code of conduct and internal awareness mechanisms.
- Regularly conducts cybersecurity awareness training and social engineering prevention drills.
- Executed 51 phishing email testing drills in 2025 and introduced the "Take 9" concept advocated by RSAC San Francisco to strengthen employee awareness, identification, and response capabilities.
- Establishes cybersecurity incident reporting and positive incentive mechanisms to encourage the proactive reporting of potential threats.

Third-Party and Supplier Cybersecurity Management

- During supplier cybersecurity risk assessments, we reference applicable SEMI E187 cybersecurity requirements based on the characteristics of the products, equipment, or services provided by the supplier, thereby strengthening third-party cybersecurity risk management.
- Implements access and compliance management for suppliers, on-site contractors, and external business partners.
- Requires suppliers, business partners, and external personnel to comply with trade secret protection and the Group's cybersecurity regulations through procurement contracts, Vendor Commitment Letters, and non-disclosure agreements (NDAs).
- Requires third-party equipment to undergo cybersecurity assessments and vulnerability scanning before connecting to the internal network, mitigating the risk of external threat infiltration and third-party collaboration.

Information Security Project: Foxconn Global Collaborative Cyber Defense and AI-Enabled Protection

In response to the Group's digital transformation and global operational footprint, Foxconn continued to advance its "Sharing, Collaboration, and Mutual Prosperity" Global Joint Defense Mechanism in 2025. By integrating resources across security monitoring, threat intelligence, incident response, and cross-regional collaboration, the Group is progressively establishing a cybersecurity protection model centered on "continuous monitoring, rapid response, and cross-regional joint defense."

With a zero-trust architecture and multi-layered defenses as its foundation, the Group continues to strengthen identity authentication, endpoint protection, network perimeter security, threat detection, and incident reporting. In parallel, the Group has introduced AI-assisted analysis, threat intelligence sharing, and a cybersecurity awareness platform to enhance capabilities in assessing anomalous events, providing early risk warnings, and enabling employees to identify threats and respond effectively, thereby mitigating the potential impact of cybersecurity incidents on global operations.

Project Highlights

Organization and Resource Deployment

Deployed a dedicated professional cybersecurity team and established the "Foxconn Cybersecurity Intelligence Sharing Alliance" to integrate internal and external intelligence exchange. In addition, the Cybersecurity Research Institute has invested in developing an AI attack lifecycle prediction model.

Zero-Trust Architecture and Multi-Layered Defense

- Network and Perimeter: Deployed next-generation firewalls (NGFW), web application firewalls (WAF), intrusion prevention systems (IPS), and DNS and DDoS protection, and introduced a next-generation secure remote access mechanism.
- Identity and Access: Established a Group-wide single sign-On (SSO) platform and comprehensively implemented multi-factor authentication (MFA) across the Group.
- Endpoint and Data: Applied data labeling and encryption controls based on confidentiality classification and deployed next-Generation anti-virus (NGAV), endpoint detection and response / managed detection and response (EDR/MDR), and network detection and response (NDR).

Proactive Risk and Vulnerability Management

Introduced an attack surface management system and an automated threat intelligence collection system. Implemented the Secure Software Development Life Cycle (SSDLC) to realize a Shift-Left Security approach, alongside conducting regular penetration testing and critical business continuity drills.

Round-the-Clock Monitoring and Reporting Mechanism

Built a centralized cloud-based Security Operations Center (SOC) that integrates system logs into a Security Information and Event Management (SIEM) platform. Through AI monitoring and correlation analysis, early-warning capabilities were strengthened, and standard procedures for incident grading, reporting, and ransomware response were refined.

Deepening Cybersecurity Culture

Introduced a cybersecurity awareness platform offering training courses across diverse scenarios and regularly conducted social engineering drills.

Project Outcomes

100 cybersecurity professionals

Deployed a dedicated professional cybersecurity team, currently comprising 100 cybersecurity professionals. Established the "Foxconn Cybersecurity Intelligence Sharing Alliance" to integrate internal and external intelligence exchange, while the Cybersecurity Research Institute invests in the R&D of an AI attack lifecycle prediction model.

7x24 Security Operations Center (SOC)

A global 24/7 Security Operations Center (SOC) has been successfully established, enabling real-time monitoring across multiple sites worldwide and creating a continuous, comprehensive defense-in-depth network.

100 % Critical Equipment Under Management and Monitoring

Under a phased deployment strategy, current asset monitoring coverage now includes the critical ICT equipment across all global campuses under management and monitoring. We will continue to expand this footprint and remain dedicated to achieving full global asset monitoring coverage.

Outperforming Industry Averages Group's Overall Exposure Level Assessment

- Through AI-driven analysis and threat intelligence sharing mechanisms, threats were successfully disrupted at an early stages of the attack chain, significantly reducing cybersecurity incident response times and enhancing all employees' ability to identify and prevent threats.
- Completed the rollout of a cybersecurity awareness platform, providing employees with multi-scenario and multilingual training courses.

Information Security Management Mechanism

Business Continuity Plan

To enhance operational resilience in the face of unexpected incidents, Foxconn has established a comprehensive business continuity management system. Through Business Impact Analysis (BIA), we inventory and identify critical business functions and formulate tailored Business Continuity Plans (BCPs) based on the Recovery Time Objective (RTO) and Recovery Point Objective (RPO). When major disasters or unexpected incidents disrupt operations, the existing BCP mechanism helps management make rapid decisions. It prioritizes employees' safety and ensures that core systems and critical operations are restored as quickly as possible, minimizing operational impact.

To verify the feasibility and executability of these plans, the Group conducts critical business continuity drills at least once a year. In 2025, the Group completed drilling and testing operations for 320 core systems, with all results meeting the expected standards. Based on drill experiences, we continuously review reporting procedures and response responsibilities, dynamically optimizing the BCP's content.

Group completed drilling and testing operations

320 core systems

Cybersecurity Vulnerability Assessment

The Group has established a comprehensive mechanism for internal and external vulnerability identification to proactively detect potential vulnerabilities and mitigate the associated risks. For internal protection, we introduced a multi-layered vulnerability scanning system that regularly scans IT assets, including operating systems, servers, and network equipment, for vulnerabilities. For external protection, we leverage a third-party cybersecurity risk assessment platform to continuously monitor the Group's global digital assets on a 24/7 basis. In 2025, the Group maintained the highest cybersecurity rating of "A" (Excellent) and remained above the manufacturing industry average; more than 40 major business groups and subsidiary entities within the Group also maintained an "A" rating.

For application security, the Group adheres to the Secure Software Development Life Cycle (SSDLC) guidelines and integrates them into its DevSecOps process to implement a shift-left security approach. This not only shortens security patching times but also uses information dashboards and cybersecurity self-inspection checklists to review the SSDLC implementation status of each project continuously. By integrating GitLab into CI/CD pipelines, the Group has fully scripted and automated source code scanning and vulnerability analysis, reducing the burden of manual testing and the risks of software development.

For identified weaknesses and risk items, the Group requires the relevant responsible units to complete patching, effectiveness verification, and subsequent tracking in accordance with established schedules. This establishes a complete, closed-loop vulnerability management system that continuously mitigates potential cybersecurity threats across systems and application environments.

Cybersecurity Monitoring, Incident Reporting, and Response Mechanism

The Group has established comprehensive standard guidelines for reporting and handling cybersecurity incidents. On the technical side, we have introduced AI-driven automated analysis and collaboration mechanisms to carry out the analysis, investigation, and response processes for cybersecurity incidents. This automatically handles repetitive tasks and connects incident reporting and management mechanisms, reducing average reporting and response times by more than 50%.

When a cybersecurity incident occurs, the involved unit must immediately conduct an initial level assessment and proceed according to the following procedures:

Immediate Reporting

Regardless of the incident level, it must be reported to the Group's IT cybersecurity team within 1 hour of discovering the incident. (Level 1 incidents are exempt from reporting if they have already been intercepted and handled by automated tools, but they must be included in the statistics.

Time-Limited Review

Level 1 or 2 incidents must be reviewed within 8 hours; Level 3 or 4 incidents must be reviewed within 2 hours.

Senior Management Reporting and Response

Level 3 or 4 incidents must be immediately reported to the CISO and CIO. The Secretariat of the Cybersecurity Governance Committee will evaluate whether to establish an Emergency Response Center (ERC) to initiate subsequent handling.

Highest-Level Reporting

If it is determined to be a Level 4 incident, the Secretariat must report it to the Chairman of the Board immediately.

By continuously strengthening multi-layered cybersecurity defense mechanisms, the Group successfully blocks an average of over **230 million** external attack attempts and malicious connections daily.

In 2025, the Group experienced no material cybersecurity incidents

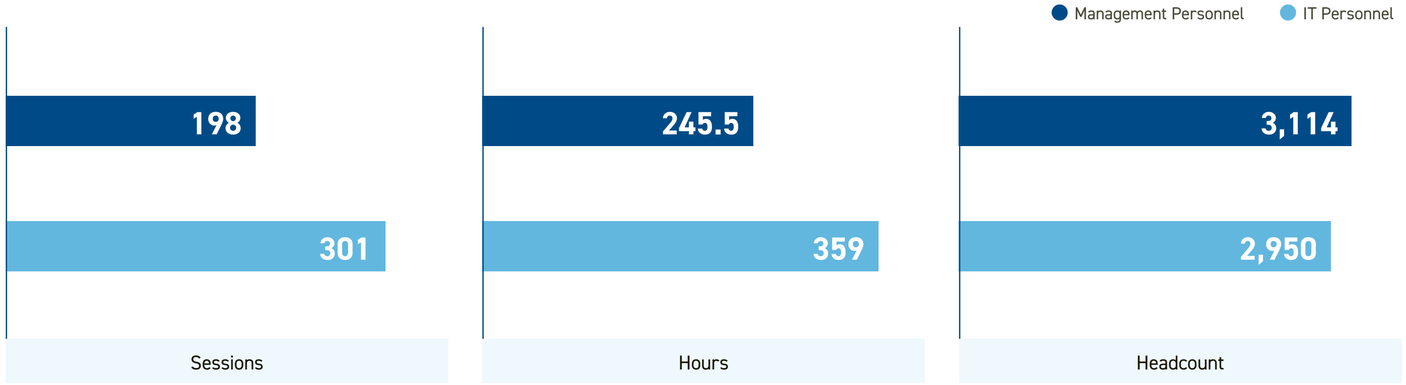
0

Employee Cybersecurity Awareness Training

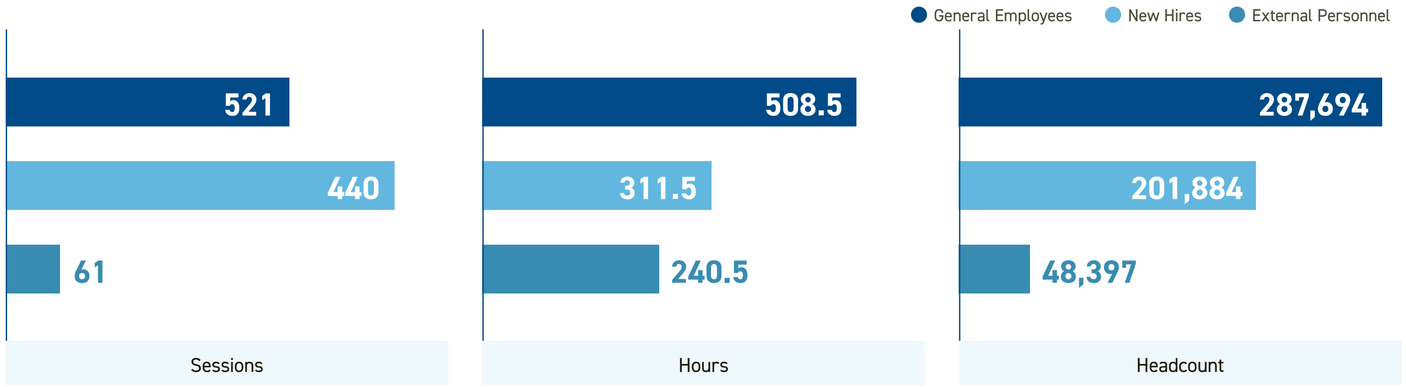
The Group has established a systematic cybersecurity training framework that enhances employee cybersecurity awareness through a tiered learning model, thereby mitigating risks arising from human error. We conduct regular training and awareness -raising activities each year. The courses cover foundational concepts of information security, advanced protection technologies, and the prevention of social engineering attacks. We arrange training topics tailored to different job requirements, enhancing personnel's cybersecurity knowledge and practical capabilities at all levels and roles. In addition to general campaigns, the Group continuously reinforces employees' awareness of identifying and reporting common cybersecurity risks through simulation drills, assessments, and targeted awareness activities.

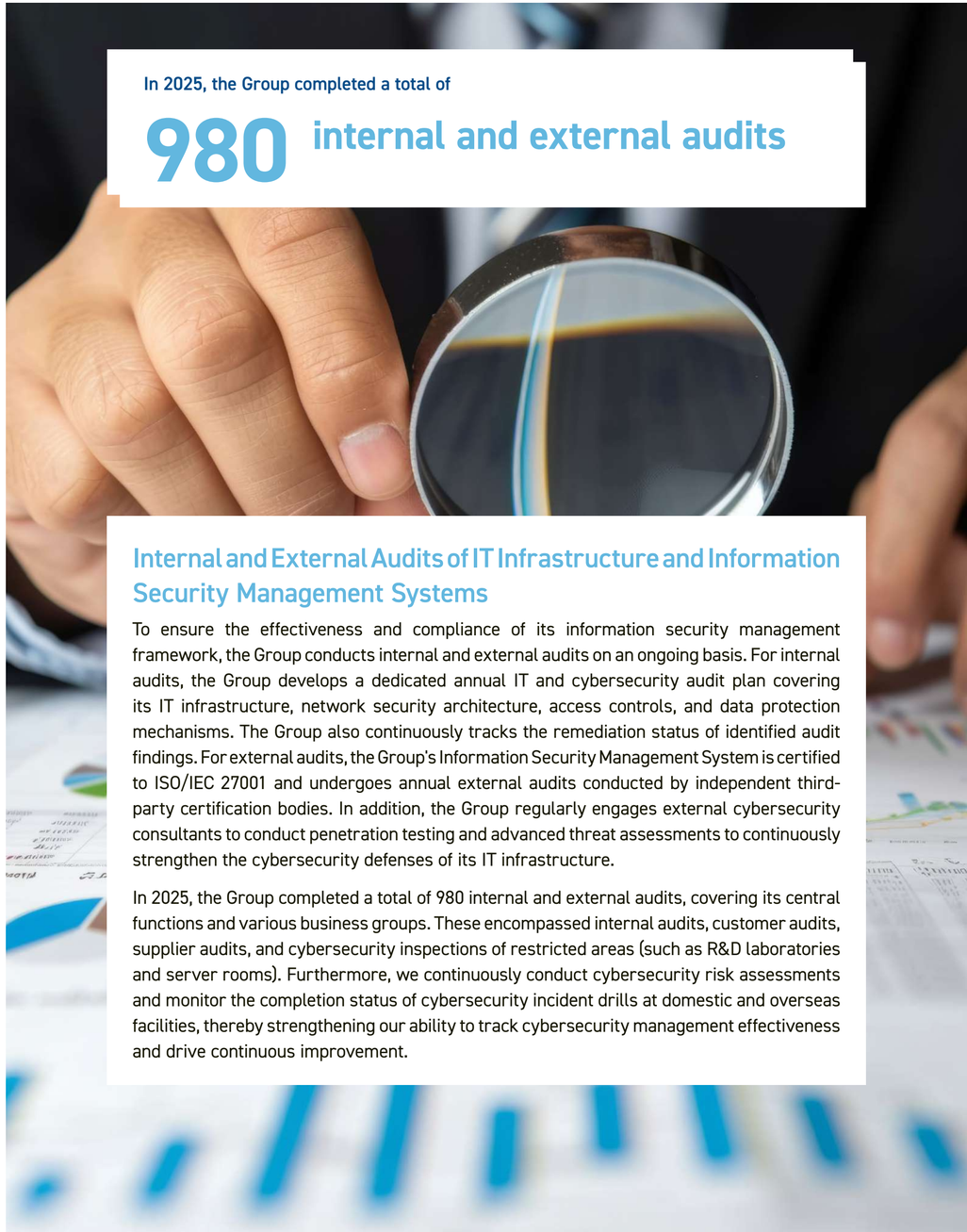
2025 Foxconn Information Security Training

▸ By Management Level



▸ By Employee Type





In 2025, the Group completed a total of

980 internal and external audits

Internal and External Audits of IT Infrastructure and Information Security Management Systems

To ensure the effectiveness and compliance of its information security management framework, the Group conducts internal and external audits on an ongoing basis. For internal audits, the Group develops a dedicated annual IT and cybersecurity audit plan covering its IT infrastructure, network security architecture, access controls, and data protection mechanisms. The Group also continuously tracks the remediation status of identified audit findings. For external audits, the Group's Information Security Management System is certified to ISO/IEC 27001 and undergoes annual external audits conducted by independent third-party certification bodies. In addition, the Group regularly engages external cybersecurity consultants to conduct penetration testing and advanced threat assessments to continuously strengthen the cybersecurity defenses of its IT infrastructure.

In 2025, the Group completed a total of 980 internal and external audits, covering its central functions and various business groups. These encompassed internal audits, customer audits, supplier audits, and cybersecurity inspections of restricted areas (such as R&D laboratories and server rooms). Furthermore, we continuously conduct cybersecurity risk assessments and monitor the completion status of cybersecurity incident drills at domestic and overseas facilities, thereby strengthening our ability to track cybersecurity management effectiveness and drive continuous improvement.

Customer Privacy Protection

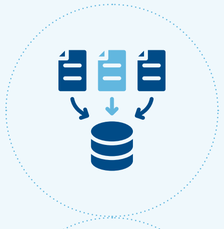
Guided by the principle of respecting and protecting personal privacy, the Group strictly complies with applicable international laws and the laws of the jurisdictions where it operates, and has formulated a comprehensive Hon Hai Technology Group Privacy Policy. This policy applies comprehensively to all of the Group's global operating sites and business activities. It further requires all suppliers, contractors, and third-party business partners to jointly comply with the relevant regulations, thereby promoting consistent privacy protection practices across the entire value chain. Beyond these policy requirements, the Group continuously strengthens each unit's understanding and execution of its privacy protection obligations through internal management processes, access controls, and educational campaigns.

To ensure the effective operation of its privacy protection mechanisms, the Group designated the Sustainability Committee as the dedicated unit for privacy matters in 2025. The Committee is responsible for coordinating the formulation, promotion, and supervision of privacy policies, as well as cross-unit coordination. In parallel, the Group has integrated its privacy policy and management system into its overall Enterprise Risk Management (ERM) and compliance management framework. We regularly identify potential privacy risks within our data processing flows and formulate corresponding mitigation and protection measures. Through regular reviews, internal audits, and improvement tracking, we continuously enhance the compliance and management consistency of our personal data processing procedures.

The Group maintains a zero-tolerance policy toward any conduct that violates privacy rights or personal data protection. If an investigation confirms involvement in an incident that breaches this policy or the relevant regulations, the Group will immediately review and improve its management measures. It will also discipline the personnel involved in accordance with applicable disciplinary regulations and, where necessary, seek compensation or pursue legal action. An employee who violates this policy will face disciplinary action commensurate with the severity of the harm caused, up to and including termination of employment or legal action; a business partner that fails to comply with this policy may have its business relationship with the Group terminated.

To establish a mechanism for continuous supervision and improvement, the Group will progressively build and refine its internal and external audit mechanisms over the short to medium term to verify the implementation level of its privacy policy. This includes incorporating privacy rights into the Group's risk management system and conducting annual risk assessments; having internal Group units conduct annual internal audits of privacy policy compliance; and continuously strengthening the privacy management system by introducing frameworks such as ISO 27001, the Privacy Information Management System. We will also periodically commission independent, professional third-party organizations to conduct external audits and verifications, continuously refining our privacy management practices and safeguarding stakeholder rights.

Foxconn Technology Group places great emphasis on customer privacy and data security. Based on the Privacy Policy, we implement the following customer data protection principles



Transparent Collection and Notification of Use

Before collecting customer information, we clearly notify customers of the nature of the information and its specific purpose, achieving genuine information transparency.

Customer Autonomy and Control

In accordance with the relevant regulations, customers may exercise their rights to opt out, give explicit consent, and request data access, data portability, data correction, and data deletion.

Data Retention Period and Security Protection

Customer information is retained only for the period necessary to fulfill the purpose of collection, after which it is securely destroyed or anonymized in accordance with the law. Throughout the retention period, mechanisms such as encryption technologies and access controls are applied to mitigate the risk of unauthorized access or leakage.

Disclosure and Sharing with Third Parties

Unless otherwise required by law, the Group will not sell, trade, or rent personal information. The Group may disclose personal data to third parties only to fulfill legal obligations, assist public agencies in carrying out their duties in accordance with the law, assert or protect the Group's legal rights, respond to requests from the personal data owner, or act within the necessary scope of the specified purpose.