



5. Corporate Governance

Management Approach

5.1 Corporate Governance

5.1.1 Board Operations

5.1.2 Ethical Management

5.1.3 Legal Compliance

5.2 Risk Management

5.2.1 Enterprise Risk Management

5.2.2 Information Security / Cybersecurity and Privacy Protection

5.2.3 Intellectual Property

5.3 Moving Toward a Sustainable Supply Chain

5.3.1 Supply Chain Management Framework and Overview

5.3.2 Supply Chain Sustainability Management

5.3.3 Conflict Minerals Management

5.4 Operating Capability

5.4.1 Operational Achievements and Future Outlook

5.4.2 Tax Policy

5.4.3 Policy Influence

Technology Clusters: Pyramid City Mission

Introduce Responsible AI (RAI) to address AI opportunities and challenges, and demonstrate a reliable and resilient sustainable management system.

Management Approach

● Above 95% ● 90%-95% ● Below 90%

Topic	Strategy	2025 Targets	2025 Results	Status	2026 Targets	2030 Targets
Corporate Governance & Ethical Management	Improve performance in global sustainability assessment	1. Maintain a top-tier ranking in the top 5% among listed companies in the Corporate Governance Evaluation 2. Maintain or improve strong performance in ESG ratings 3. Achieve at least 20% representation of directors of different genders on the Board 4. Link executive officer compensation to ESG performance indicators 5. Increase the attendance rate of individual directors at each term to 80%	1. Ranked in the top 5% of listed companies in the Corporate Governance Evaluation 2. Maintained or improved strong performance in ESG ratings 3. Achieved 20% female representation on the Board 4. Established linkage between executive officer compensation and ESG performance indicators 5. All directors achieved an individual attendance rate of 100% in 2025	●	1. Maintain a top-tier ranking (top 5% among listed companies) in the Corporate Governance Evaluation 2. Maintain or improve strong performance in ESG ratings 3. Achieve at least 20% representation of directors of different genders on the Board 4. Link executive compensation to ESG performance indicators 5. Ensure individual director attendance rates reach at least 80% per term	1. Maintain a top-tier ranking in the top 5% among listed companies in the Corporate Governance Evaluation 2. Maintain or improve ESG ratings and performance 3. Achieve at least one-third representation of directors of different genders on the Board 4. Link executive compensation to ESG performance indicators 5. Ensure individual director attendance rates reach at least 80% per term
	Implement employee training to strengthen the Code of Conduct and foster a culture of integrity and ethical business practices	Achieve a 100% signing rate of Code of Conduct Statement	100%	●	100%	100%
Risk and Crisis Management	Regularly identify the risk appetite for all levels of the Company	1. Establish a global Key Risk Indicator (KRI) dashboard to enhance proactive risk monitoring and early warning capabilities 2. No material risk events involving amounts over NT\$100 million occurred under the enterprise risk management system	0 case(s)	●	1. Integrate risk databases, incorporating risk assessment questionnaires covering sustainability, climate, and anti-corruption-related risks 2. Conduct risk sensitivity analyses and stress testing 3. Continue to manage and mitigate the likelihood of significant risk events that could affect the Company, defined as events involving property losses exceeding NT\$100 million	Continue to manage and mitigate the likelihood of significant risk events that could affect the Company, defined as events involving property losses exceeding NT\$100 million
		Conduct regular self-assessments of internal controls and achieve a reliability coefficient $\geq$ 95%	ICS (Internal Controls Self-assessment) 99.94% (1H) ; 99.84% (2H) ICE (Internal Controls Evaluation) 99.98%	●	Conduct regular self-assessments of internal controls and achieve a reliability coefficient $\geq$ 95%	Conduct regular self-assessments of internal controls and achieve a reliability coefficient $\geq$ 95%

Management Approach

● Above 95% ● 90%-95% ● Below 90%

Topic	Strategy	2025 Targets	2025 Results	Status	2026 Targets	2030 Targets
Corporate Governance & Ethical Management	Establish a regulatory compliance system and regularly review domestic and international regulatory changes relevant to operations to ensure all business activities comply with applicable laws and regulations	Employees No material violations of laws (fines exceeding NT\$1 million)	Employees No material violations of laws (fines exceeding NT\$1 million)	●	Employees No material violations of laws (fines exceeding NT\$1 million)	Employees No material violations of laws (fines exceeding NT\$1 million)
		Shareholder/Securities Related Matters 1. Complied with all regulations without incurring any penalties 2. Closely monitor regulatory or policy changes issued by competent authorities and adjust internal management practices accordingly	Shareholder/Securities Related Matters 1. Complied with all regulations without incurring any penalties 2. Closely monitored regulatory and policy changes issued by competent authorities and adjusted internal management practices accordingly. 3. Completed compliance training for all internal managers	●	Shareholder/Securities Related Matters 1. Complied with all regulations without incurring any penalties 2. Closely monitor regulatory or policy changes issued by competent authorities and adjust internal management practices accordingly 3. Regulatory compliance training for all internal managers	Shareholder/Securities Related Matters 1. Complied with all regulations without incurring any penalties 2. Closely monitor regulatory or policy changes issued by competent authorities and adjust internal management practices accordingly
		Environmental Health and Safety 1. Stay up to date with regulatory developments, remain compliant, and incur no major penalties (fines exceeding NT\$1 million) 2. Regularly conduct EHS (Environment, Health, and Safety) regulatory identification and adjust internal procedures in a timely manner	Environmental Health and Safety 1. Stayed up to date with regulatory developments, remain compliant, and incur no major penalties (fines exceeding NT\$1 million) 2. Regularly conduct EHS (Environment, Health, and Safety) regulatory identification and adjust internal procedures in a timely manner	●	Environmental Health and Safety 1. Stay up to date with regulatory developments, remain compliant, and incur no major penalties (fines exceeding NT\$1 million) 2. Regularly conduct EHS (Environment, Health, and Safety) regulatory identification and adjust internal procedures in a timely manner	Environmental Health and Safety 1. Stay up to date with regulatory developments, remain compliant, and incur no major penalties (fines exceeding NT\$1 million) 2. Regularly conduct EHS (Environment, Health, and Safety) regulatory identification and adjust internal procedures in a timely manner
		Customer/Supplier/Litigation/Patent/ Trademark Achieve 95% digitalization of contract and intellectual property asset management; continuously monitor international regulatory trends and customer needs to respond and adapt accordingly	Customer/Supplier/Litigation/Patent/ Trademark contract and intellectual property asset management digitalization reached 95%	●	Customer/Supplier/Litigation/Patent/ Trademark Achieve 100% digitalization of contract and intellectual property asset management; continuously monitor international regulatory trends and customer needs to respond and adapt accordingly	Customer/Supplier/Litigation/Patent/ Trademark In addition to the digitalization of contracts and intellectual property asset management, as well as the continuous monitoring of international regulatory trends and customer needs for timely responses and adjustments, big data analytics will also be applied to the database to serve as a strategic reference for future planning
Information Security/ Cybersecurity & Privacy	Establish an updated information security/cybersecurity system and mechanism to ensure information security for the Company and its customers	The facility passed the customer information security compliance assessment. Certification rate:100%	100%	●	100%	100%
		100% of the facility has obtained ISO/IEC 27001 certification coverage	100%	●	The headquarters office and all manufacturing facilities have achieved 100% ISO 27001 certification and continue to maintain their validity through regular updates	The headquarters office and all manufacturing facilities have achieved 100% ISO 27001 certification and continue to maintain their validity through regular updates

Management Approach

● Above 95% ● 90%-95% ● Below 90%

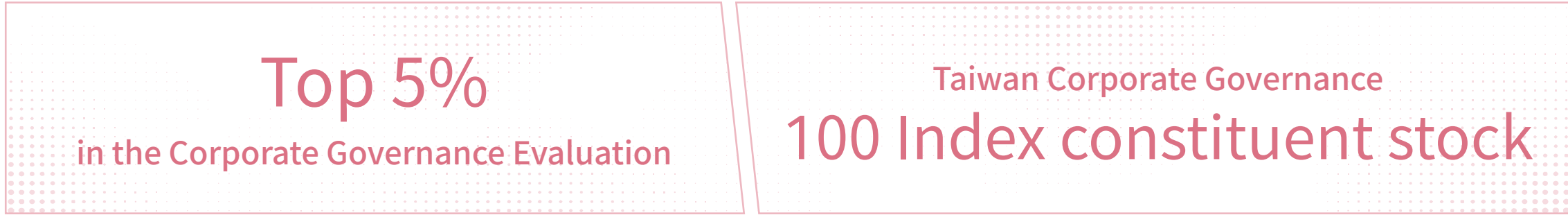
Topic	Strategy	2025 Targets	2025 Results	Status	2026 Targets	2030 Targets
Supplier Sustainability Management	Strengthen Supply Chain Sustainable Resilience	Risk identification 1. Tier 1 suppliers' compliance rate:100% 2. Critical non-tier 1 suppliers' compliance rate:100%	Tier 1 suppliers' compliance rate 100% Critical non-tier 1 suppliers' compliance rate 100%	●	Risk identification 1. Tier 1 suppliers' compliance rate:100% 2. Critical non-tier 1 suppliers' compliance rate:100%	Risk identification 1. Tier 1 suppliers' compliance rate:100% 2. Critical non-tier 1 suppliers' compliance rate:100%
		Ratio of sustainability audit on high-risk suppliers:100%	100%	●	100%	100%
		Improvement and guidance of audit deficiency for high-risk suppliers NCR completion rate:100%	100%	●	100%	100%
Supplier Sustainability Management	Deepen Regional & Strategic Cooperation ¹	Machinery and materials in the China Site >98%	98.05%	●	> 98%	> 98%
		Machinery and materials in the Vietnam site >50%	54.24%	●	> 55%	> 70%
	Signature of Major Statements	100% Declaration signing rate of the Supplier Code of Conduct for tier 1 suppliers	100%	●	100%	100%
		100% Declaration signing rate of the “Declaration of Non-use of Conflict Minerals”	100%	●	100%	100%
	Optimize Strategy Supplier Core Competitiveness	Greenhouse gas reduction and water source inventory coverage >67%	90.11%	●	>90%	>90%
		Suppliers with high energy consuming material obtaining GHG external verification (ISO 14064-1): ≥ 75%	96.15%	●	≥ 70% of critical materials suppliers	≥ 85%
		Suppliers with high energy consuming material obtaining energy management system external verification (ISO 50001): ≥ 65%	82.69%	●	100%	100%

Note :

1. Optimize the regional supply chain: The percentage of local procurement is based on Wistron’s key manufacturing sites at major operational locations, including five major facilities in mainland China and one in Vietnam, and reflects purchases made from suppliers within those respective regions.

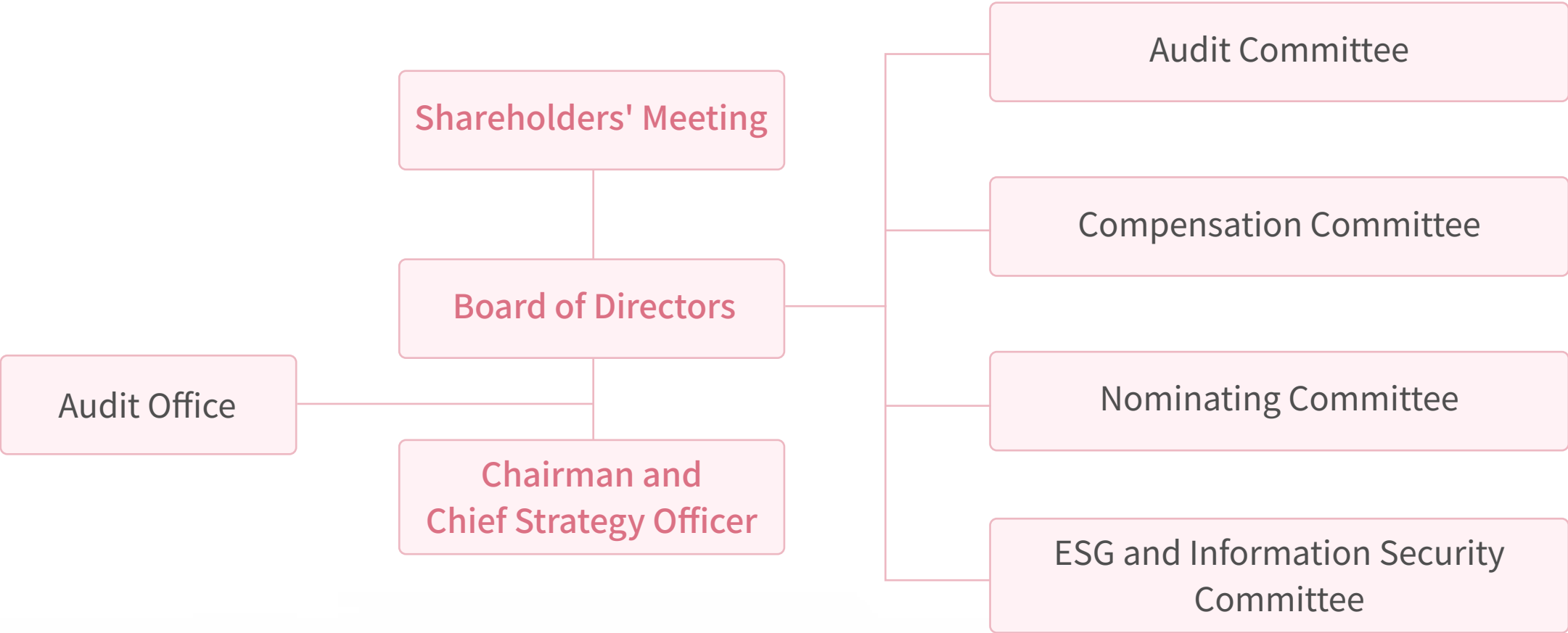
2. Signing rate of the “Declaration of Non-use of Conflict Minerals” excludes logistics providers.

5.1 Corporate Governance



Wistron believes that sound corporate governance is the foundation of corporate sustainability. The Company is committed to establishing an effective governance framework based on principles of protecting shareholder rights, strengthening Board functions, respecting stakeholder interests, and enhancing information transparency. In accordance with Article 277 of the Company Act, amendments to the Articles of Incorporation must be approved by shareholders at a general meeting, ensuring their participation in major corporate decisions. The scope of directors’ responsibilities is not subject to limitation, as stipulated by relevant provisions of the Company Act. Wistron continuously implements various policies and mechanisms to enhance governance quality, maximize shareholder value, and ensure sustainable operations.

5.1.1 Board Operations



The Board of Directors serves as Wistron’s highest governing body, responsible for overseeing the management team to ensure compliance with applicable laws and regulations while enhancing information transparency. Leveraging their professional expertise, board members provide strategic guidance on major decisions to prevent the implementation of policies that could undermine the Company’s value. They also emphasize the cultivation of a culture rooted in integrity and ethical conduct, fulfilling corporate responsibilities to support sustainable operations and protect shareholder interests. The management team also regularly reports to the Board of Directors on the Company’s operational status, development strategies, and key sustainability- and risk-related matters, including updates on sustainability initiatives and progress, the implementation of ethical business practices, information security measures, material topics, stakeholder engagement, and the operation and implementation of risk management activities. This helps maintain smooth and effective communication between management and the Board. For details of Board-management communications and significant resolutions, please refer to the [Company’s Annual Report](#). In compliance with governance guidelines, the Board of Directors convenes at least once per quarter and held a total of nine meetings in 2025. The average attendance rate among board members reached 100%, surpassing Wistron’s requirement of an annual attendance rate of at least 80%.

Functional Committee

To strengthen the Board’s supervisory function and enhance management effectiveness, Wistron has established four functional committees under the Board: the Audit Committee, the Compensation Committee, the Nominating Committee, and the ESG and Information Security Committee (formerly the Sustainability Committee). The operational status of each functional committee is detailed in the table below. For further information, please refer to [Wistron's Annual Report](#).

Committee	Function	Members	Attendance rate (excl. proxy)	Major Resolutions
Audit Committee	Oversees the fair presentation of Wistron’s financial statements; the appointment, dismissal, independence, and performance of Certified Public Accountants; the effective implementation of internal controls; compliance with applicable laws and regulations; and the control of existing or potential risks.	Independent Director Mr. Chien-Hsin Chuang Independent Director Mr. Jack Chen Independent Director Mr. S.J. Paul Chien Independent Director Ms. Pei-Pei Yu Independent Director Ms. Mei-Ling Chen	100%	• Annual & quarterly financial statements • Major investment and CapEx • Major loans, endorsements & guarantees • Risk management reports
Compensation Committee	Establishes and periodically reviews the policies, systems, standards, and structures for performance evaluation and compensation of directors and managers, and regularly evaluates and sets the compensation for directors and managers.	Independent Director Mr. S.J. Paul Chien Independent Director Mr. Jack Chen Independent Director Ms. Pei-Pei Yu	100%	• Recommendations on director remuneration • Recommendations on performance bonuses & salary adjustments for managers • Recommendations on percentage of management salary to employee remuneration
Nominating Committee	Selects and reviews qualified candidates for directors, managers, and members of Board committees, and establishes and periodically reviews the structure and functioning of Board committees.	Independent Director Ms. Pei-Pei Yu, Chairman Mr. Simon Lin Independent Director Mr. Jack Chen Independent Director Ms. Mei-Ling Chen	100%	• Recommendations on changes in management appointments • Established the CEO Succession Plan • Organized training for directors
ESG and Information Security Committee *	Formulates the direction and objectives for corporate social responsibility, sustainability, and information security, and oversees related policies, implementation plans, and performance.	Director, President & CEO Mr. Jeff Lin Director Philip Peng Independent Director Ms. Mei-Ling Chen	100%	• Reviewed progress to sustainability targets & set future goals • Established the Corporate Governance Policy, Information Security Policy, and the Anti-Corruption and Anti-Bribery Policy • Revised Wistron’s Code of Conduct, ESG and Information Security Committee Charter, Sustainable Development Best Practice Principles, Sustainability Report Preparation and Assurance Management Guidelines, and Sustainability Information Management Guidelines • Work reports from the Sustainability Office and Information Security Executive Committee • Reported on ethical management, material sustainability topics and stakeholder communication • Completed GHG inventory and verification for all subsidiaries

Note: On April 2, 2025, the Company’s ESG Committee was renamed to ESG and Information Security Committee. The composition of committee members was also revised, replacing senior executives and independent directors with board members, and requiring the participation of at least one independent director.

Composition and Diversity of the Board of Directors

In accordance with the [Articles of Incorporation](#), the Company shall have seven to nine directors, each serving a three-year term. A candidate nomination system is adopted, and directors are elected by the shareholders’ meeting from a list of nominated candidates to safeguard shareholders’ rights and interests. The Company has stipulated a Board diversity policy in Article 20 of its [Corporate Governance Best Practice Principles](#), stating that the composition of the Board should consider multiple aspects, including gender, nationality, culture, professional background, and industry experience. For specific management objectives and progress regarding board member diversity, please visit our [website](#).

Wistron’s Board of Directors currently consists of nine members, all of whom are highly respected professionals with extensive experience in the industry. Following the re-election upon the expiration of their term in 2024, the average board tenure is nine years. Two members (22%) also serve as company executives, and five seats (56%) are held by independent directors, all of whom meet the independence requirements set forth in the “Regulations Governing Appointment of Independent Directors and Compliance Matters for Public Companies,” and have not exceeded the three-term limit. The Board also includes two female directors, accounting for 22%. For information on the procedures related to the election of Board members, please visit Wistron’s [website](#). In addition, none of the Company’s directors concurrently serve as directors at more than four other publicly listed companies. Comprehensive information on each Board member—including educational and professional background, concurrent positions in other companies, attendance records, and other relevant details—is disclosed in the [Company's annual report](#) and on its [official website](#).

The Chairman of the Board is elected by the Board of Directors and serves as the leader of the Board internally and the Company’s representative externally. To uphold the Board’s intent and enhance decision-making efficiency, the Chairman also serves as the Chief Strategy Officer, responsible for strategic planning, development, implementation, and long-term corporate growth. In the event of any proposals involving conflicts of interest, the Chairman abstains from participation in accordance with the principle of avoidance.

Director Training and Performance Evaluation

To enhance directors’ knowledge and competencies in areas such as regulations, economics, environment, social issues, and risk management, the Company arranges annual training courses for Board members. In 2025, Board members underwent an average of nine hours of training, covering topics such as “Current Global Economic Trends and the Implications of the Trump Administration’s New Policies,” which explored recent developments in the global economy and the impact of Trump-era policies on trade systems and exchange rate movements, and “Cybersecurity Governance and Management in a Geopolitical Context,” which helped directors understand cybersecurity operational risks and international cybersecurity strategies amid geopolitical developments, thereby supporting the formulation of cybersecurity governance policies. In addition, to ensure regulatory compliance, the Company also provided an online training course on insider trading prevention regulations for all directors and managers.

To ensure effective corporate governance and enhance the performance of the Board of Directors, Wistron conducts annual performance evaluations of the Board and its functional committees in accordance with the [Rules for Board of Directors and Functional Committee Performance Assessments](#). These evaluations encompass key areas, including legal compliance, corporate governance, risk management, and sustainable development goals, to ensure that the Board and its committees fulfill their responsibilities across all ESG dimensions. The evaluation results serve as a basis for determining compensation and for the continuous enhancement of the Board’s operations and effectiveness. In 2025, performance evaluations were conducted for the Board of Directors, Audit Committee, Compensation Committee, Nominating Committee, and ESG and Information Security Committee. Upon completion of the scoring and analysis, the performance evaluation scores for the Board of Directors and its functional committees were 99.83, 99.80, 100, 100, and 100, respectively. All results were rated as “Exceeds Standards” and have been reported to the Board and each respective committee. In addition, the Company commissions an external professional independent organization or team of external experts and scholars to conduct a Board performance evaluation at least once every three years. In 2025, the Company engaged the Corporate Governance Association to carry out an external evaluation of the Board. The results provided positive affirmation regarding the Board structure, interaction and communication between the management team and the Board, ESG achievements, and talent development and succession planning.

For detailed information on the Company’s director training and Board performance evaluation reports, please refer to the [Company's annual report](#) and on its [official website](#).

Conflicts of Interest Management

For agenda items that may involve conflicts of interest for Directors or the legal entities they represent, compliance with Article 15 of the Rules and Procedures of Board of Directors Meetings is required. In such instances, Directors must disclose the relevant details of the conflict during the meeting. If their participation in discussions or voting may compromise the Company’s interests, they are required to abstain and recuse themselves. Additionally, they are prohibited from exercising voting rights on behalf of other Directors. If a Director’s spouse, relatives within the second degree of kinship, or a company under the Director’s control has a vested interest in the meeting agendas, the Director is considered to have a personal interest in the matter.

For details on the execution of director recusals from conflict-of-interest agenda items in 2025, concurrent directorships held by Board members, cross-shareholdings with suppliers or other stakeholders, the existence of controlling shareholders, and information on related parties, their relationships, transactions, and outstanding balances, please refer to the [Company's annual report](#).

Compensation Policy for the Board of Directors and Senior Executives

The compensation for the Company’s directors includes remuneration and business execution expenses. In accordance with Articles 11 and 16 of the Articles of Incorporation, director remuneration is allocated from an amount not exceeding 1% of the Company’s annual profit. Reasonable compensation is granted based on the Company’s operating results and the individual director’s contribution. All payments are made in accordance with the Guidelines for Director and Functional Committee Remuneration and are subject to prior approval by the Compensation Committee and the Board of Directors. To strengthen the alignment between director compensation and sustainability performance, the Company has established the ESG and Information Security Committee, which regularly incorporates sustainability issues into the Board’s meeting agendas and decision-making processes. For directors who concurrently serve as the President & CEO, sustainability-related performance indicators have been included as key performance metrics. Additionally, the Company’s annual Board performance evaluations incorporate “sustainable strategy implementation and sustainability performance” as one of the assessment criteria, reinforcing director involvement in the Company’s sustainable development efforts and serving as a reference for determining remuneration.

The compensation package for senior executives/managers includes remuneration, retirement and pension benefits, holiday bonuses, and employee remuneration (in the form of cash or stock). Among these, bonuses, compensation (cash/stock), and stock options are variable components and represent the primary portion of executive remuneration. Senior executives are also entitled to legally mandated insurance and retirement plans. The compensation of senior executives/managers is based on individual performance and is reviewed and assessed by the Compensation Committee. Recommendations are submitted to the Board of Directors for approval prior to execution.

Linking Incentive Systems and Sustainable Performance

To encourage senior executives, key professional talent, and all employees to focus on long-term, comprehensive performance and achieve sustainable business objectives, Wistron has progressively incorporated the objectives of its ESG 6-pillar and key performance indicators related to material sustainability issues into the short- and long-term incentive compensation mechanisms for the President & CEO, senior executives, and business unit heads since 2022. This approach links sustainability performance with overall business performance and ensures that sustainability considerations are effectively integrated into corporate operational decision-making. In 2026, sustainability-related performance indicators for the President & CEO cover the governance, environmental, and social dimensions. For governance, the focus is on a sustainable supply base. Beyond supporting suppliers in strengthening their decarbonization capabilities, collaborative action plans have been advanced across the supply chain to drive collective progress. For environmental issues, the indicators address climate change through the increased use of recycled and renewable materials in green products, expansion into waste battery recycling, and greater adoption of renewable energy across global operations. These efforts contribute to carbon emissions reduction, alignment with the Science Based Targets initiative (SBTi), and achievement of the 1.5° C target pathway. For the social dimension, the indicators focus on reducing occupational disasters and increasing employee engagement. The relevant sustainability performance indicators are assigned to the responsible executive officer for each pillar of the ESG 6-pillar strategy, as well as to the corresponding business unit heads, who are tasked with developing and implementing the indicators.

Sustainability Performance Indicators			President & CEO	Business Unit Managers (Including main BG head)	Executive Officers (including heads of the ESG 6-pillar working groups)
Governance	Sustainable Supply Chain	Strengthen decarbonization efforts across the supply chain to increase carbon reductions	3%	15%	10%
Environmental	Green Products/ Product Development and Innovation	Increase revenue generated from products containing recycled or renewable materials	4%	15-20%	25%
	Circular Economy	Increase the shipment of recycled plastics and commercialize battery recycling solutions	1%	30%	5%
	Climate Strategy and Energy Management	Reduce electricity intensity	–	10-15%	10%
		Increase use of renewable energy	10%*		
	Water Resource Management	Reduce water usage intensity	–		
Social	Talent Attraction and Retention	Increase employee engagement and reduce turnover rate	1%	10-15%	5%
	Occupational Health and Safety	Reduce occupational injuries and increase employee satisfaction	2%	10-15%	5%

Note: 4% for the President & CEO and 6% for the Chief Sustainability Officer.

Presented on a weighted basis

5.1.2 Ethical Management Policies and Organization

To establish a unified set of values and culture across all personnel, Wistron has adopted a [Code of Conduct](#), approved by the Board of Directors, as the highest standard of behavior for all employees of the Company, its subsidiaries, and joint ventures in which the Company holds significant impact. This Code serves as a guiding framework for all business activities. The global human resources and administrative departments hold primary authority and responsibility for implementing this Code, as well as establishing necessary procedures to ensure compliance.

To uphold ethical business practices, Wistron has established the [Code of Ethical Conduct](#), the [Ethical Corporate Management Best Practice Principles](#), and the [Corporate Governance Best Practice Principles](#). These policies require all employees to fully understand and comply with professional ethical standards, respect and strictly adhere to confidentiality agreements with clients, and refrain from accepting gifts or special treatment without proper cause. Wistron also engages customers, suppliers, business partners, and other stakeholders to promote a shared understanding of and commitment to the Company’s core values of integrity. The implementation status of integrity management is reported and reviewed annually by the Global Human Resources and Administration Division to the Board of Directors, the highest management body, at the end of each year.

Anti-Corruption Risk Management and Due Diligence

To ensure the transparency and effectiveness of its anti-corruption risk management mechanisms, Wistron has established a Board-approved [Anti-Corruption and Anti-Bribery Policy](#), which expressly prohibits all forms of bribery and improper benefits. The Company has also established reporting, investigation, and internal control mechanisms to prevent corruption risks and uphold business integrity. In addition, Wistron launched a project in 2025 to implement the ISO 37001 Anti-Bribery Management System. The initial certification scope covers supply chain management-related processes at the corporate headquarters. The Company passed external verification in June 2026 and plans to strengthen its culture of compliance through annual external surveillance audits.

In 2025, Wistron conducted anti-corruption and anti-bribery risk assessments across all global operating sites (100% coverage). Among 28 identified risk categories, two medium- to high-risk categories were identified: Supplier Management and Designated Supplier Procurement Management. To mitigate and effectively control potential corruption and bribery risks, the Company developed and implemented three action plans.

Internally, the Company identifies Treasury Management & Corporate Communications, Global Supply Chain Management, and Administration Services as potential high-risk areas. These departments are subject to internal audit or periodic job rotations. Additionally, managerial staff in these functions are required to attend external training programs offered by professional institutions to enhance their understanding of legal compliance.

Externally, before establishing business relationships with agents, suppliers, customers, or other partners, the Company assesses the legality of their business practices, the presence of integrity-related policies, and any history of unethical conduct. During the course of business, Wistron communicates its integrity management policy and related internal regulations in accordance with internal procedures. Contract terms include requirements to comply with Wistron’s anti-corruption policies, which cover reasonable and transparent payment terms, the handling of misconduct, and violations related to commissions, kickbacks, or other improper benefits. Wistron maintains a firm stance against offering, promising, requesting, or accepting any form of improper advantage, whether directly or indirectly. If unethical behavior is identified, business dealings are immediately terminated, and the entity is blacklisted.

Personnel Risk Assessment and Due Diligence Process

Step & Stage	Description	Risk Rating/Actions
1 Classification and preliminary assessment	- Responsible unit compiles personnel list for all departments - Conduct stage one assessment according to job-related risks, reputation, and conflict of interest	Stage 1 Assessment Determine preliminary risk level
	- Determine risk level of all personnel based on preliminary assessment results - Low Risk: Review once every five years - Medium/High Risk: Initiate stage two of the due diligence process, which includes in-depth review of government or business relationships and records of unusual conduct	Low risk Review once every five years Medium/High risk Initiate stage two of the due diligence process
3 Risk mitigation and review	- High-risk personnel are required to complete advanced training and sign a Code of Conduct acknowledgment - The responsible unit shall review the effectiveness of risk controls - For those where risk is deemed unmanageable, terminate employment or suspend promotions	Actions for high-risk personnel Training & signing of a Code of Conduct acknowledgment Review by responsible unit; termination or suspension of promotion where risk is deemed unmanageable

Business Partner Risk Assessment and Due Diligence Process

Step & Stage	Description	Risk Rating/Actions
1 Supplier classification and screening	- Identify supplier’s operational status - Based on transaction amount, frequency, and technical importance, label significant suppliers - Distinguish between Tier-1 suppliers and non-Tier-1 suppliers (customer-designated or indirect suppliers)	Significant suppliers Tier-1 vs. non-Tier-1
2 Risk assessment	- Significant Tier-1 suppliers are rated on five dimensions: Company background, reputation, delivery, government relations, and transaction procedures - Identify risk level (low, medium, or high) based on rating	Five dimensions → Classification as low, medium, or high risk
3 Due diligence	- Medium-risk vendors: General due diligence - High-risk vendors: Enhanced due diligence - If general due diligence reveals poor reputation or unusual government relations, upgrade to high-risk	Medium risk General due diligence High risk Enhanced due diligence
4 Risk mitigation and review	- Implement mitigation measures such as awareness campaigns, training, signing of commitment letters, or audits - Assess the effectiveness of mitigation measures in controlling risks - The responsible unit shall review the effectiveness of controls and conduct regular reviews	Mitigation measures Awareness campaigns, training, commitment letters, audits Regular review by responsible unit

Commitment and Support

To ensure that all personnel fully understand relevant regulations and expectations, Wistron continuously implements education, training, and awareness programs. All members of the Board of Directors signed the Code of Conduct Acknowledgment Form, and dedicated training sessions on the prevention of insider trading have been arranged to reinforce their corporate governance responsibilities in upholding integrity. For all new employees, the Company requires reading and signing the [Code of Conduct](#) Acknowledgment Form and completing an online ethics training course. In 2025, both the acknowledgment and training completion rates reached 100%. For existing employees, annual training on the Code of Conduct, including anti-corruption, anti-bribery, and anti-competitive practices, is mandatory for all personnel across all facilities. In 2025, the training completion rate for all employees was also 100%, reflecting Wistron’s strong commitment to promoting a culture of integrity.

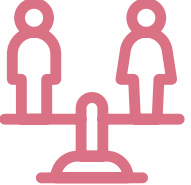
Code of Conduct Training and Acknowledgment

Item	2022	2023	2024	2025
Code of Conduct Signing Rate (%)	100%	100%	100%	100%
New Employee Training Coverage Rate (%)	100%	100%	100%	100%
Regular Training Coverage Rate for All Employees (%)	100%	100%	100%	100%
Training Completion Rate for All Employees (%)	100%	100%	100%	100%

Category	Code of Conduct Training Rate	Taiwan	Overseas
Years of Service	New Employees	3,785 (100%)	8,992 (100%)
	Current Employees	13,618 (100%)	33,035 (100%)
Employment Type	Direct employees	7,320 (100%)	31,786 (100%)
	Indirect employees	10,083 (100%)	10,241 (100%)
Location	Administrative	6,998 (100%)	27 (100%)
	Manufacturing	10,405 (100%)	42,000 (100%)

Whistleblowing and Disciplinary Measures

Internal and external stakeholders are encouraged to contact the Global Human Resources and Administration Division for any questions regarding the Code of Conduct. For different categories of issues, Wistron has also established reporting and inquiry channels (as shown in table below) to communicate with internal and external stakeholders.

Category	 Ethical Management	 Workplace Equality	 Employee Feedback	 On-site Inquiries	 Regulations & Safety
Channel	Reporting channel for corruption & ethics; President & CEO mailbox	Sexual harassment reporting channel; discrimination and harassment hotline	Employee suggestion box; QR code suggestion box; HR e-suggestion box	Employee hotline; employee relations specialists; employee representative meetings	Privacy protection hotline; emergency hotline; whistleblowing
Medium	Email, hotline, website	Hotline, extension line, email, written report	Physical suggestion box, QR code form, mobile application	Extension line, face-to-face communication, in-person meeting	Extension line, written report, email
Relevant Topics	Business ethics, corruption, violation of ethical conduct, human rights protection, environmental protection	Sexual harassment, workplace bullying, discrimination, unfair treatment	Labor relations, workplace environment, personal rights, feedback on management	Work arrangements, frontline management, psychological counseling, inquiry on salary and benefits	Violations of Wistron’s Privacy Policy, occupational safety and health, and emergency situations
Target	Internal employees & external stakeholders (i.e., suppliers, customers etc.)	Internal employees	Internal employees	Internal employees	Internal employees & external stakeholders
Responsible Unit	Office of the President & Global Human Resources and Administration	Human Resources Department, Grievance Committee	Human Resources Department, Administration Department	Human Resources Department (employee relations), Labor Union/Labor Relations Committee	Legal/compliance departments, work safety departments

Institutionalizing a Culture of Integrity through the Grievance and Reporting System

Wistron encourages all employees and external stakeholders to report unethical conduct or violations of business ethics through its whistleblowing channels. The Company is committed to maintaining the confidentiality of whistleblower identities and report contents to ensure whistleblowers are protected from any form of retaliation or unfair treatment. The Company enforces a zero-tolerance policy toward any violations of the Code, including retaliation against whistleblowers, and will take disciplinary action in accordance with the [Code of Conduct](#).

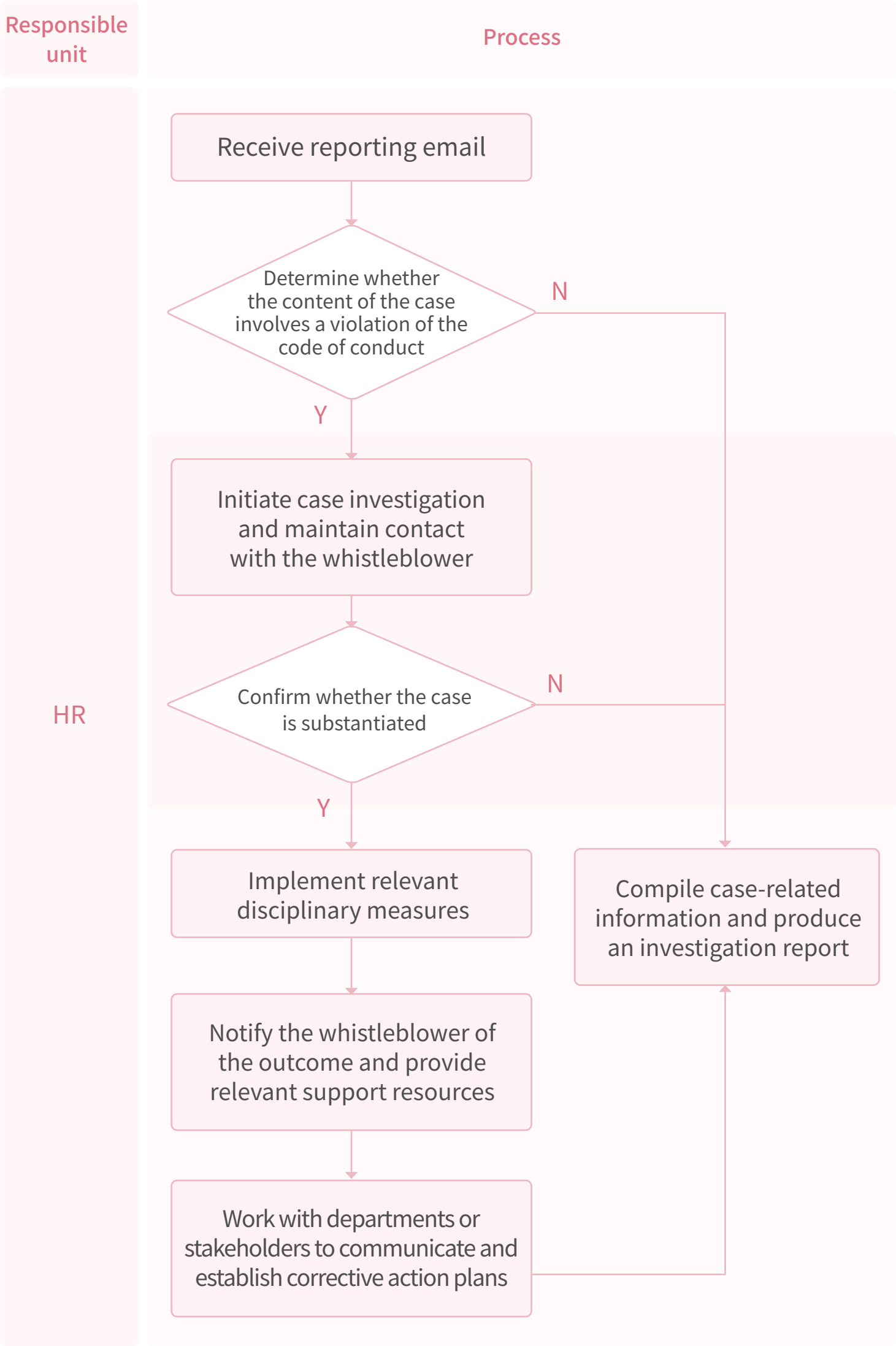
To ensure employees are familiar with the whistleblowing channels and related mechanisms, Wistron includes relevant information in onboarding and Code of Conduct training. The Company also promotes awareness through public information boards and the internal website, educating employees on when and how to report, available reporting channels, processing procedures, and whistleblower rights. This fosters a proactive culture of integrity and strengthens the Company’s whistleblowing system.

The Company maintains dedicated email and reporting platform channels for whistleblowing and grievance reporting. Cases involving violations of the Code of Conduct are primarily handled by the Global Human Resources and Administration Division, with investigation and handling procedures outlined in the diagram on the next page. A quarterly summary of case-handling progress is reported to the Independent Directors, and an annual report on case handling is submitted to the Board of Directors. The Audit Division is responsible for overseeing the investigation and resolution process.

Code of Conduct Reports / Number of Substantiated Cases		2022	2023	2024	2025	
		Number of Substantiated Cases			Number of Reports	Number of Substantiated Reports
Business Ethics and Operations	Corruption and Bribery	0	0	0	3	1
	Conflicts of Interest	0	0	0	0	0
	Fair Trading	0	0	0	0	0
	Money Laundering or Insider Trading	0	0	0	1	0
	Trade Secrets	0	1	1	0	0
	Privacy/Personal Data Protection	0	0	0	0	0
	Other (Political Contributions, Charitable Contributions, and Social Engagement)	0	0	0	9	1
	Total Number of Business Ethics and Operational-Related Cases	0	1	1	13	2
Protection of Human Rights	Discrimination	0	0	0	1	0
	Harassment/Misconduct	3	1	0	6	0
	Occupational Health and Safety	0	1	0	1	0
	Total Number of Human Rights–Related Cases	3	2	0	8	0
Environmental Protection	Total Number of Environmental Protection–Related Cases	0	0	0	0	0
Total		3	3	1	21	2

Note: One corruption case was substantiated through report investigations between 2022 and 2025. However, there were no confirmed convictions or administrative sanctions for corruption during this period.

Summary of 2025 Grievances & Reports: Investigation and Outcomes



Category	Location/Case Details/Summary of Investigation	Outcome
Corruption and Bribery	HQ/Procurement Allegation that a supplier colluded with a Wistron buyer for improper gain → No substantiating evidence found	Closed
	HQ Allegation that a supervisor accepted bribes from an equipment supplier in exchange for providing tender information → No substantiating evidence found	Closed
	Chongqing Site Supervisor falsely reported bonus payments → Substantiated	Major demerit & reassignment
Money Laundering or Insider Trading	Taiwan Office Employee suspected of insider trading → Reported allegations were inconsistent with findings	Closed
Other	HQ Insufficient transparency regarding the procurement of data center equipment → Responsible contact informed and project status communicated to the supplier	Closed
	Kunshan Site Outstanding payment dispute related to electrostatic garment transactions from 2004–2005 → No relevant internal records available and the complainant was unable to provide supporting evidence	Provisionally closed
	Texas Site Alleged non-compliance with SOPs → Investigation found no evidence supporting the allegation	Closed
	Allegation that a contract worker falsified information during the recruitment process → No current employee matching the reported circumstances was identified	Closed
	HQ Allegation that Wistron used unauthorized software → Usage was found to be compliant with licensing requirements	Closed
	Hsinchu Site Recycling contractor suspected of infringing upon Wistron’s interests → Insufficient key evidence to substantiate the allegation	Provisionally closed
	Texas Site Suspected non-compliance involving contractor-supplier relationships and material handling procedures → Insufficient critical evidence to substantiate the allegation	Provisionally closed
	Chongqing Site Employee stole and sold company property for personal gain → Substantiated	Dismissed & handed over to the police
	Malaysia Site Employee reported for applying and paying unreasonable facility fees of factory registration → No evidence of non-compliance was identified	Closed
Discrimination	Mexico Site Alleged unreasonable rejection of an external applicant → Complainant was a former employee who was not eligible for rehire due to unsatisfactory performance	Closed
Harassment/ Misconduct	Taiwan Office Supervisor assigned excessive workloads and obstructed leave arrangements before an employee’s departure → Resolved through intervention and communication by secondary management	Closed upon resolution
	Taiwan Office Employee alleged unlawful dismissal → Investigation confirmed that the employee had committed serious violations of the Code of Conduct and other company regulations; dismissal procedures were compliant	Closed
	Kaohsiung Opto-Electronics Male employee alleged to have harassed a female employee → Investigation found no intent to harass, and the female employee stated that no inappropriate conduct had occurred	Provisionally closed
	Taiwan Office Supplier allegation of bullying by Wistron supervisor → Resolved through communication between both parties’ management teams	Closed upon resolution
	Hsinchu Site Complaint regarding poor attitude by a security guard → None was identified; additional training and discipline imposed afterward	Strengthened training
	Hsinchu Site Allegation of improper management practices by a supervisor → Investigation determined the complaint had been filed under another employee’s name without authorization; the employee concerned did not wish to pursue a complaint	Closed
Occupational Health and Safety	Hsinchu Site Employee failed to comply with designated smoking area requirements → Additional no-smoking signage installed, security patrols strengthened, and plant-wide announcements made	Strengthened management measures

Key Issues in Ethical Management

Anti-Competitive Practices

Integrity in business is a fundamental corporate social responsibility. Wistron has established the [Ethical Corporate Management Best Practice Principles](#), requiring all employees to conduct business activities in accordance with fair competition laws. Employees are prohibited from engaging in price-fixing, bid rigging, production or quota restrictions, or market sharing and allocation practices based on customers, suppliers, geographic areas, or types of business. Wistron strictly adheres to all applicable laws in business operations and incorporates topics related to fair trade into Code of Conduct training to ensure that all employees understand relevant regulations. From 2022 to 2025, the Company has not been penalized by authorities for anti-competitive conduct or monopolistic practices, and monetary losses due to lawsuits related to anti-competition laws were zero.

Political and Charitable Contributions

Under the Company’s Code of Conduct, all political contributions—direct or indirect—by employees to political parties or politically active organizations or individuals must comply with the following principles:

1. Comply with applicable laws and regulations; contributions may not be used to seek business or transactional advantages. Any legitimate political donations made in Wistron’s name, regardless of amount, must be approved by the Chairman.
2. Employees may not, without authorization, make political contributions on behalf of the Company.
3. Company property, facilities, or work hours may not be used for any political activities.

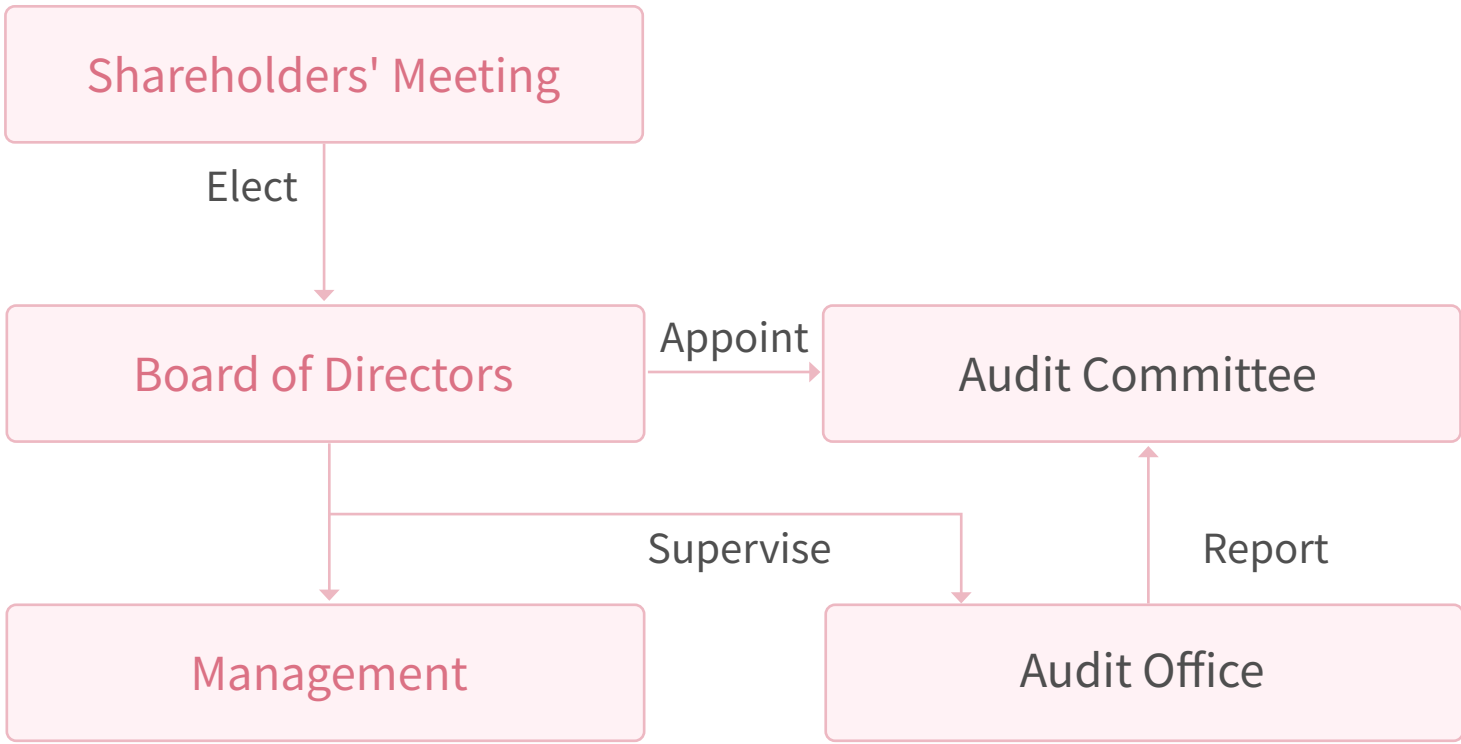
From 2022 to 2025, the Company did not make any political contributions. However, Wistron respects employees’ freedom of political expression and encourages them to fulfill their civic responsibilities.

In terms of public welfare and charitable giving, all donations and sponsorships are governed by internal management regulations, which strictly prohibit disguised bribery or personal gain. These rules ensure compliance with anti-corruption standards and legal requirements.

Internal Control and Internal Audit

Internal Audit Organization

Wistron’s Board of Directors has established an Audit Committee composed entirely of independent directors, supported by an independent internal Audit Department that reports directly to both the Board and the Audit Committee. The Head of Internal Audit not only regularly attends and reports at Audit Committee and Board meetings, but may also report directly to the Chairman and the Audit Committee as necessary to ensure audit independence and communication.



Note: The Internal Audit Department is staffed with qualified and competent audit professionals.

Audit Objectives

Through risk assessments, system reviews, and on-site inspections, the Internal Audit Department assists various departments in identifying opportunities for process improvement and securing their cooperation in implementing self-improvement initiatives. These efforts help enhance overall business performance and create greater value for shareholders and stakeholders.

Audit Operations

At the end of each year, the Internal Audit Department conducts a risk assessment based on changes in the operating environment, regional characteristics of subsidiaries, future business strategies, and the results of prior audits. Based on this assessment, the department prepares the annual audit plan for the following year, which is submitted to the Audit Committee for review and then approved by the Board of Directors for implementation. If circumstances change during the execution of the audit plan, adjustments are made as needed, subject to approval by the Board of Directors.

Monthly	Quarterly
Audit findings are reported in writing to the Audit Committee; matters requiring clarification are communicated separately when necessary.	1. Key audit findings are reported to senior management and presented to the Board of Directors. 2. External auditors (CPAs) are invited to present findings from their review of financial statements and engage in two-way communication with independent directors, as well as the heads of finance and internal audit.

Audit Management of Subsidiaries

In consideration of local legal requirements and the operational nature of each subsidiary, Wistron supervises and guides subsidiaries to establish appropriate control measures for oversight and management as needed. All subsidiaries are included within the scope of internal audits. Audit activities are carried out based on risk assessment results. For any internal control deficiencies or irregularities identified by the Internal Audit Department, thorough communication is conducted with the audited units, which are required to propose specific and effective corrective measures. The Internal Audit Department continues to follow up on these issues until full resolution is achieved.

Self-Assessment of Internal Controls

Wistron’s internal control system is designed by management in accordance with the “Regulations Governing the Establishment of Internal Control Systems by Public Companies” and approved by the Board of Directors, with consideration of the Company’s overall operations.

The internal control system consists of key components and control activities intended to reasonably ensure the achievement of the following objectives:

1. Operational effectiveness and efficiency
2. Reliability, timeliness, transparency, and regulatory compliance of reporting
3. Compliance with applicable laws and regulations

The internal control system adopts a digital platform for self-assessment operations. The President & CEO supervises and encourages all internal departments and subsidiaries to conduct self-assessments on their internal controls at least once per year. The Internal Audit Department reviews these self-assessment reports, together with the status of improvements to any deficiencies or irregularities previously identified through audit activities. This comprehensive review forms the primary basis for the Chairman and the President & CEO to assess the overall effectiveness of the internal control system and to issue the Internal Control System Statement.

The Internal Audit Department conducts evaluations in accordance with the “Internal Auditing Implementation Rules” to assess the adequacy of the internal control system and the effectiveness of its implementation in day-to-day operations. Both ongoing and project-based audits are conducted, encompassing all internal operations and subsidiaries of the Company. Based on the results of risk assessments, the Internal Audit Department develops an annual audit plan, which is reviewed and approved by the Board of Directors and subsequently implemented. Monthly audit reports are reviewed by the Audit Committee, and identified deficiencies are continuously tracked until corrective actions are completed. On a quarterly basis, the Head of Internal Audit attends Audit Committee and Board meetings to report audit findings. Through the effective implementation of the internal control system, Wistron did not identify any material internal control deficiencies in 2025.

2025 Achievements

Through effective implementation of internal controls,
no major internal control deficiencies found.

5.1.3 Legal Compliance

Wistron has established a comprehensive set of internal operational procedures in accordance with relevant regulations governing public companies. The Company continuously monitors regulatory updates from competent authorities and promptly adjusts internal policies as needed, requiring all subsidiaries within the Group to comply and ensure lawful operations.

In addition, the management team closely monitors domestic and international policies and regulations that may affect the Company’s financials and business operations. In response, the Company not only adjusts its risk management procedures accordingly but also promptly updates related training programs to reflect the latest regulatory requirements. The Training Center is responsible for coordinating these programs and engaging internal and external professional instructors. Training initiatives include, but are not limited to, onboarding programs, compliance training for managers and legal personnel, and company-wide compliance education. Post-training evaluations, such as exams or surveys, are conducted to ensure learning effectiveness. Through continuous education and training, the Company strengthens employees’ legal awareness and professional capabilities, ensuring compliance with applicable regulations in customer interactions.

Regarding legal compliance, in 2025, the Company did not incur any fines exceeding NT\$1 million per case that would have a material impact on operations due to violations of applicable laws or regulations (on topics including but not limited to product safety, marketing, communications, and business ethics).



5.2 Risk Management

Wistron adheres to a philosophy of sustainable operations. Through the establishment, implementation, and maintenance of proactive risk management mechanisms, the Company continuously monitors internal and external issues and environmental changes. It conducts operational impact analyses and develops effective and flexible responses to address challenges. Regular self-assessment and ongoing improvements enhance the Company’s resilience, fulfilling its commitment to uninterrupted operations and safeguarding the best interests of customers and stakeholders. Additionally, Wistron effectively manages operational risks and fosters a risk-aware culture through continuous optimization of education and training, performance management, risk assessment, early warning notifications, and public disclosures.

5.2.1 Enterprise Risk Management

Risk Governance Structure

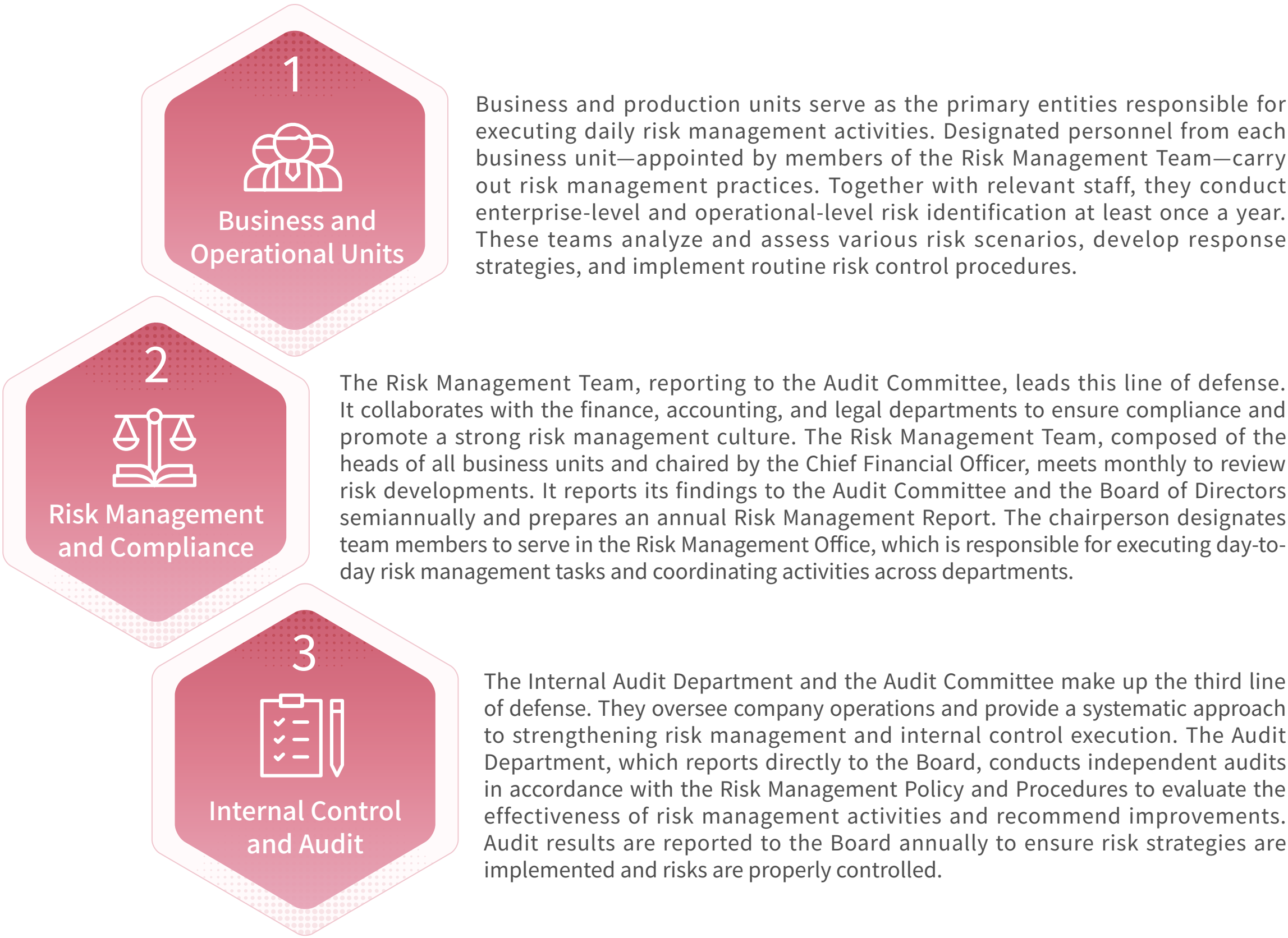
Wistron adheres to the principles outlined in ISO 31000 – Risk Management Guidelines and adopts the “Three Lines of Defense” framework to systematically assess and manage potential risks that could impact business operations. With active involvement from the Board of Directors, the Company ensures comprehensive risk governance. In 2023, the Board of Directors approved the [Risk Management Policy and Procedures](#), which formally integrates risk management into operational activities and daily management processes to achieve the Company’s risk management objectives.

Board Oversight Responsibilities

The Board of Directors is the highest supervisory body for risk management at Wistron. It is responsible for approving risk management policies and related guidelines, ensuring effective implementation of the risk management framework. To fulfill its supervisory duties, the Board authorizes the Audit Committee to assist in overseeing the risk management mechanisms and their implementation. The Audit Committee reviews the effectiveness of risk management operations annually, provides recommendations for improvement, and reports to the Board to ensure strategic goals are met and stakeholder interests are protected.

Three Lines of Defense Framework

Wistron adopts the Three Lines of Defense model to establish a multi-level, structured risk control mechanism that enhances internal controls and corporate governance. Responsibilities are clearly defined and coordinated across the organization to improve overall risk management effectiveness:



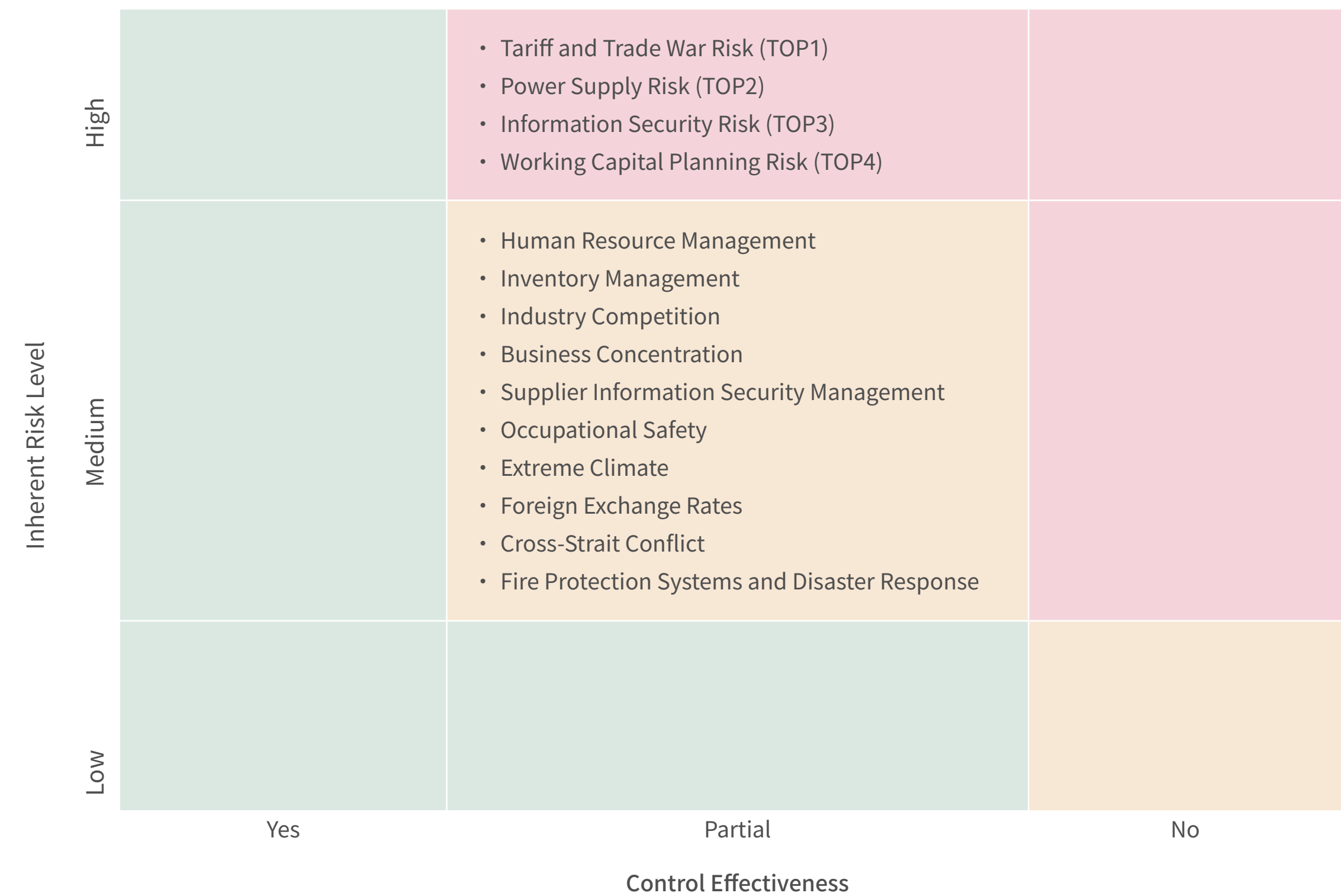
Risk Management Procedures

Wistron has established a comprehensive risk management process encompassing the following stages: risk identification, risk analysis, risk evaluation, risk response and monitoring, and risk reporting and disclosure. This systematic approach enables the Company to effectively identify, assess, and respond to various types of risks, ensuring business continuity and optimal allocation of resources. Each year, the Risk Management Team requests the respective risk management working groups to evaluate and discuss potential and emerging risks based on indicators such as likelihood of occurrence, severity of impact, and effectiveness of existing controls. The results are regularly reported to the Audit Committee and the Board of Directors.



Risk Identification

In 2025, the Risk Management Team conducted a risk assessment using structured questionnaires, taking into account the likelihood of occurrence, severity of impact, and effectiveness of existing controls. A total of 14 key medium-to-high-level risks were identified. Among these, four annual risks were assessed with a residual risk level of T – Take Immediate Action (requiring immediate remediation), and 10 were rated as I – Improve Controls (requiring improvements to controls or response measures).



- Monitor Assurance (Safe zone; maintain current controls)
 - Improve Controls (Moderate risk; improve controls or response measures)
 - Take Immediate Action (Severe risk; take immediate action)
- Top 4 risks selected after senior-level approval
 - A total of 23 effectively controlled risks fall within the green area

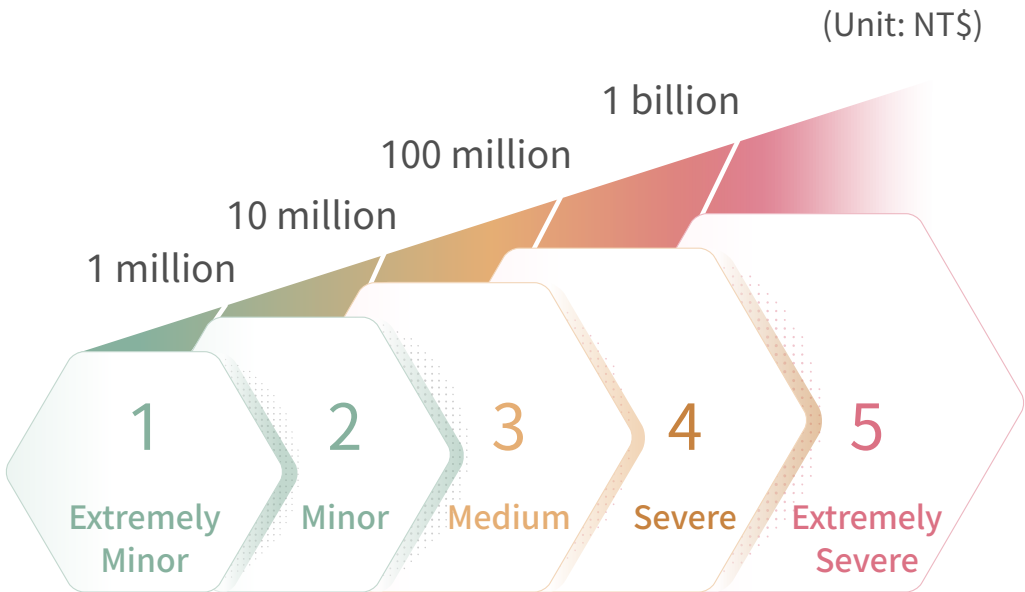
Risk Sensitivity Analysis and Stress Testing

To strengthen the Company’s risk awareness, the Company regularly conducts sensitivity analyses and stress tests on significant risks that may affect its operations. Through risk sensitivity analyses, Wistron is able to quantify the financial impacts of various risks. Additionally, stress testing allows Wistron to assess its resilience through extreme scenarios by simulating extreme risks and volatility. Through these analyses and tests, the Company is able to more comprehensively assess, manage, and respond to a wide range of risks, thereby ensuring stable operations and supporting sustainable development.

Types of Risk	Scenario Analysis	Results of Sensitivity Analysis and Stress Testing
Foreign Exchange Risk	The Company’s exchange rate risk primarily arises from foreign-currency-denominated cash, accounts receivable, borrowings, accounts payable, and other assets, which may result in foreign exchange gains or losses upon conversion. The major foreign currency exposures are in USD and CNY.	Based on the position calculation as of December 31, 2025, if the New Taiwan Dollar appreciates or depreciates by 2% against the U.S. dollar and Chinese yuan, the Company’s 2025 net income after tax would change by approximately NT\$1 billion, reaching a level classified by the Company as having an extremely significant impact.
Interest Rate Risk	Interest rate risk is assessed based on the Company’s total outstanding liabilities and their remaining maturity.	Based on total liabilities as of December 31, 2025, a change in interest rates of ±300 basis points would affect the Company’s 2025 net income after tax by approximately NT\$1 billion, which would constitute an extremely significant impact as defined by the Company.
Geopolitical Risk	In the event of escalating geopolitical tensions affecting production sites in Taiwan and Mainland China, the Company estimates potential business interruption losses by simulating factory shutdown durations.	If a production halt extends to 30 days, the resulting business interruption loss would exceed NT\$1 billion, reaching the Company’s threshold for an extremely significant impact.

Risk Appetite

The Risk Management Team defines the Company’s annual risk appetite based on strategic objectives and the balance between risk and return. Once approved by the Audit Committee and the Board of Directors, the defined risk appetite is communicated and implemented across all business units. Risk appetite is categorized into five levels, each corresponding to a defined range of potential financial loss. These levels are linked to specific preventive and mitigation measures, ensuring that all critical risks are effectively managed.



Risk Prioritization, Response, and Monitoring

Senior management and the Risk Management Team convene semiannual risk meetings to regularly review the implementation results of risk management activities and discuss and prioritize the risks facing the Company. Following assessment, Wistron identified the top three risks for 2025: tariff and trade war risks, power supply risks, and information security risks. For the risks identified above, the responsible units develop corresponding risk response action plans. Following review and confirmation by the respective unit heads, these plans are incorporated into the Audit Committee’s and Board of Directors’ regular risk governance process for identification, monitoring, and review.

Types of Risk	Description of Risk	Mitigation Measures	Assessment Method
Geopolitical Risk	With the return of tariff policies under the Trump 2.0 era and the accelerated push for “Made in America,” global supply chains face increasingly severe challenges. The US government continues to threaten higher import tariffs to encourage the reshoring of manufacturing activities and strengthen domestic production capacity.	1. Regularly review geopolitical issues relevant to the company’s operations or those of its business partners’ locations. 2. Regularly evaluate the impact of internal and external environmental factors, and adjust production capacity accordingly to ensure optimal allocation based on customer demand. This approach reduces reliance on any single region, mitigates geographic risks, and enhances production flexibility. 3. Promote production automation to enhance manufacturing efficiency and adaptability to changing environments, thereby mitigating the operational impact of geopolitical risks.	The return of tariff policies under the Trump administration has accelerated implementation of the “Made in America” agenda, causing significant disruptions to global trade dynamics. These measures aim to reduce U.S. trade deficits with other countries and, through tariff policies, encourage other countries to renegotiate their trade agreements with the U.S. At the same time, as the U.S. continues to promote “Made in America,” companies seeking access to the U.S. market may need to invest locally. Such policies expose businesses to potential tariff costs, as well as the challenges of establishing and operating manufacturing facilities in the U.S. Failure to adjust production footprints in a timely manner or strengthen R&D and automation capabilities could result in significant financial impacts, including increased tariff and production costs, with potential losses estimated to exceed NT\$1 billion.
Power Supply Risk	The rapid growth of AI technologies requires substantial power resources. Insufficient power supply affecting either the Company or its customers could adversely impact Wistron operations.	1. Establish dedicated extra-high-voltage substations. 2. Deploy backup power infrastructure (e.g., fuel cells and generators). 3. Strengthen coordination with government authorities and power suppliers to ensure supply stability and secure priority access where applicable.	As artificial intelligence (AI) technologies continue to advance, power supply has become increasingly important to the Company's operations. High-performance computing, large language model training, and data center operations that AI requires all depend on reliable and efficient power infrastructure. Insufficient power supply may directly disrupt product testing processes and delay delivery schedules, leading to customer dissatisfaction and potential business losses to competitors, thereby affecting revenue and market share. Beyond affecting operations, unstable power supply may result in substantial financial losses arising from production interruptions, testing delays, and reputational damage, all of which may have profound impacts on Wistron’s long-term development. If not effectively managed, the potential financial impact could exceed NT\$1 billion, posing significant risks to the Company’s operational stability and ability to scale.
Operational disruptions caused by cybersecurity risks	The absence of a fully implemented Zero Trust cybersecurity framework limits visibility into the overall maturity of Zero Trust adoption. In addition, insufficient AI governance structures, organizational responsibilities, management processes, and protection mechanisms increase the risk of improper use or leakage of sensitive information.	1. Enhance Zero Trust cybersecurity defenses by implementing multiple initiatives based on scope and criticality. 2. Enhance AI governance mechanisms by implementing a range of AI governance initiatives based on scope and criticality. 3. Prohibit the use of USBs entirely, with usage permitted only through formal approval procedures. 4. Prohibit the use of external email systems.	In recent years, rapid advancements in generative AI technologies have provided hackers with increasingly sophisticated tools for malicious attacks. Social engineering tactics have evolved significantly, and the scope of attack continues to broaden. Generative AI eliminates language barriers and reduces grammatical errors in phishing emails and fraudulent messages, making them appear more credible. In addition, hackers may use generative AI to automatically collect target information and conduct highly personalized whaling attacks directed at senior executives. These developments make employee awareness training alone insufficient as a risk mitigation measure. If such incidents occur, the Company could face ransomware losses exceeding NT\$1 billion, along with negative domestic and international media coverage that may have adverse impacts on Wistron.

Emerging Risk Management

Since 2020, Wistron has annually referenced the latest external risk insights—such as the World Economic Forum’s Global Risks Report—to systematically identify emerging risks through four key procedures: understanding the industry context, conducting risk assessments (including identification, analysis, and evaluation), implementing risk treatment, and performing ongoing monitoring and review. By broadly gathering professional insights from management, Wistron proactively identifies potential emerging risks, formulates appropriate mitigation measures, and reports to the Audit Committee and the Board of Directors on a regular basis to ensure the Company can implement forward-looking response strategies.

Based on the Risk Management Team’s latest assessments conducted between the end of 2025 and early 2026, Wistron has identified war-related risks, potential overinvestment in AI infrastructure risks, AI infrastructure bottleneck risks, and tariff policy risks as its key emerging risks. The Company will continue to closely monitor the development trends and potential impacts of these risks to ensure that its risk management and control measures remain forward-looking and adaptive.

Internal and External Audits of Enterprise Risk Management

Wistron has established a robust internal and external audit mechanism to ensure the effectiveness and compliance of its risk management system. For internal audits, the Audit Department is responsible for developing the annual audit plan and conducting audits in accordance with risk-based principles, while reviewing the compliance and effectiveness of risk management activities. Audit results and recommendations for improvement are reported regularly to the Board of Directors and the Audit Committee. In addition, Wistron engages a qualified third-party professional institution every two years to assess the design and implementation effectiveness of its risk management system. The results of these assessments are incorporated into improvement plans to ensure alignment with international standards and the continuous enhancement of the system. Findings from both internal and external audits are reviewed by senior management and regularly reported to the Audit Committee and the Board of Directors. Through ongoing monitoring and oversight mechanisms, the Company further enhances the long-term effectiveness and resilience of its risk management system.



Shaping a Risk Management Culture

Wistron places strong emphasis on fostering risk awareness across all levels of the organization. In addition to conducting company-wide training on risk-related topics, Wistron integrates risk management into daily operations by aligning it closely with performance evaluation indicators to embed risk culture into the corporate culture.

Incentive Mechanisms for Risk Management

Wistron has established differentiated performance evaluation standards for employees at various levels, incorporating key risk indicators, such as human capital management and information security, into the scope of performance assessments to ensure the effective implementation of risk management.



Wistron closely integrates risk management with performance evaluation, with a particular focus on the management outcomes of specific risk areas such as human capital, to ensure effective control and continuous improvement of related risks. For senior executives, the Company has incorporated management indicators such as employee engagement/satisfaction, turnover rate, and occupational injury rate into annual performance objectives. Through these measurable performance targets, the Company ensures the stability and engagement of its human capital. Moreover, the Company regularly assesses results in these areas, and the achievement of related performance indicators serves as a key basis for determining compensation. This approach reinforces a positive feedback loop between risk management performance and incentive outcomes.

Wistron incorporates information security and cybersecurity as a key risk area in its performance evaluation framework to ensure accountability and proactive management. For example, in the area of human capital, management indicators for mid-level and junior managers are cascaded from senior executives and allocated based on departmental responsibilities. These include specific metrics such as “employee engagement/satisfaction,” “turnover rate,” and “work injury rate,” and are subject to regular performance evaluations. Through this top-down breakdown of indicators and performance monitoring, Wistron ensures that accountability for human capital management is effectively implemented at all organizational levels.

Wistron is committed to integrating information security risk controls into its performance appraisal framework to ensure that risk awareness is fully embedded at every level of the organization. To reduce the impact of information security risks on business operations, the Company conducts employee training programs and simulated social engineering exercises to strengthen awareness and alertness. Additionally, violations of information security and cybersecurity policies by departmental employees are factored into the performance appraisal indicators of department heads. Individual violations are directly reflected in each employee’s performance appraisal rating, reinforcing accountability and promoting a culture of security awareness.

To encourage all employees to actively participate in risk management, the Company has established an incentive mechanism aligned with its risk management objectives by incorporating the identification, reporting, and mitigation of significant risks into its performance evaluation and reward system. Employees who proactively identify potential risks that may affect operations, safety, quality, information security, or other significant risk events in the course of their daily work, and who promptly report such risks, propose effective mitigation measures, or contribute to reducing the likelihood or impact of those risks, are eligible for recognition and rewards, including financial incentives, provided that their contributions are assessed to have generated tangible risk management benefits.

Based on employees’ contributions to risk management—including the proactive identification of risk factors and recommendations for risk mitigation measures—the Company provides both non-financial recognition and financial rewards in accordance with the Employee Rewards and Disciplinary Regulations. By linking risk management performance with employee performance evaluations and incentive programs, the Company encourages employees to embrace the principle of “identify early, report early, and mitigate early.” Through fostering a strong risk-aware culture, the Company aims to minimize the potential impact of risks on its operations.

In addition, for significant risk issues identified by the Company, such as human capital and information security, relevant risk management indicators are incorporated into the performance evaluation criteria for managers at different organizational levels. Through the integration of performance assessments and financial incentive mechanisms, the Company encourages management to continuously promote risk mitigation initiatives, ensuring that significant risks are effectively managed while further strengthening the Company’s resilience and long-term sustainable development.

Risk Management Training

In accordance with Article 16 of the Company’s Corporate Governance Policy, Wistron provides annual risk management training for all members of the Board of Directors. The training covers the Company’s risk management principles and is designed to continually strengthen the Board’s risk management capabilities. All Board members completed risk management training in 2025.

In addition, Wistron has embedded risk management throughout its employee training framework, not only to enhance risk awareness across the workforce but also to strengthen organizational resilience and competitiveness. In 2025, the Company adopted a variety of training methods covering employees at all levels—from frontline personnel to senior management—across both Wistron and its subsidiaries. The program was designed to comprehensively enhance employees’ risk management capabilities and practical application skills. Through this annual and systematic training program, a total of 44,253 participants were recorded across global operations, representing 7,376 cumulative training hours.

Training content covered a broad range of topics, including risk management fundamentals, the development and application of risk management frameworks, emerging risk identification, and function-specific risk management case studies. Course content was closely aligned with practical business needs, ensuring that employees not only understand risk management concepts but are also able to apply them effectively in their day-to-day responsibilities.

As the global business environment continues to evolve rapidly, risk management has become a core competency for all employees, extending beyond individual functions and departments. Accordingly, the training program emphasizes the principle of “from awareness to action,” encouraging all employees to actively contribute to the shaping of a risk management culture. Looking ahead, Wistron will continue to enhance its training programs by incorporating additional risk management topics and emerging risk trends, ensuring that employees maintain a forward-looking mindset and a high level of risk awareness in an increasingly dynamic external environment, thereby supporting the Company’s long-term sustainability.

Integrating Risk Criteria into Product and Service Development

Wistron incorporates risk criteria across all stages of product and service development to systematically assess the severity of potential impacts, ensuring quality and regulatory compliance. During the development phase, Failure Mode and Effects Analysis (FMEA) and a “lessons learned” database are used to assess potential risks. In the design phase, factory personnel are involved to ensure that designs meet Design for Excellence (DFX) requirements. In the production phase, defective products are analyzed and corrective actions are implemented to reduce manufacturing risks. In the verification phase, product functionality, compatibility, and reliability are tested to ensure compliance with international and environmental standards.

Risk Reporting Mechanism

In addition to actively promoting employee awareness of risk, Wistron has clearly defined its organizational structure and role responsibilities, ensuring that all employees are integrated into the risk management framework. Employees can report potential risks through various channels, including the “President’s Mailbox,” “Employee Opinion Box,” “Employee Complaint Hotline,” and “On-site Interviews with Production Line Counselors,” to help mitigate the impact of internal and external risks. The Company has also revised its “Implementation Guidelines for Employee Rewards and Penalties” to recognize employees who propose effective risk mitigation, occupational safety, health, or environmental improvement initiatives. Recognition methods include verbal commendations, written acknowledgments, and formal awards, all of which encourage active participation in risk management efforts.



Business Continuity and Emergency Response

Wistron is committed to establishing a robust Business Continuity Plan (BCP) to ensure strong operational resilience and safeguard employee and customer interests in the face of various emergency events. To achieve this, we actively conduct a wide range of emergency response drills across our global manufacturing sites. Key features of our approach include:

- 1. **Comprehensive risk coverage:** Our drills encompass a broad spectrum of scenarios, including natural disasters (e.g., earthquakes and typhoons), human-caused incidents (e.g., fires and terrorist attacks), biosafety events (e.g., epidemic prevention and control), chemical spills, and utility disruptions involving water and power systems. In addition, as we are in the digital age, contingency plans have been established for telecommunications and network outages, workforce shortages, and labor disputes.
- 2. **Combination of practical drills and tabletop exercises:** Each site adopts a dual-track approach consisting of both practical drills and tabletop exercises based on its geographic conditions and nature of operations. For example, most sites conduct at least one live drill annually for natural disasters and fire emergencies. Under specific scenarios (pandemics, chemical and waste spills, and occupational injury prevention), certain sites also conduct enhanced annual training programs to ensure emergency response procedures are fully embedded in daily management practices.
- 3. **Resilience of critical resources:** To strengthen supply chain resilience, we conduct simulations involving material shortages and supply disruptions, enhancing the Company’s ability to allocate resources and maintain operations during periods of extreme market volatility.

To further enhance organizational resilience, in addition to conducting BCP exercises for various scenarios, Wistron has clearly defined post-disaster recovery responsibilities across departments to ensure employee safety is protected immediately following an incident and that production and services can be restored as quickly as possible.



5.2.2 Information Security/Cybersecurity and Privacy Protection

Wistron upholds the mission of building a resilient, secure, and trustworthy enterprise, regarding information security as a fundamental pillar supporting sustainable operations and digital transformation. The Company continues to implement comprehensive information security management mechanisms to safeguard the integrity, availability, and confidentiality of all information processing, while strengthening the security of information systems, devices, and network environments to mitigate potential operational risks. To enhance organizational cybersecurity resilience, Wistron regularly conducts information security drills and training, reinforcing employees’ awareness of security risks and their capacity to respond effectively. Through these measures, the Company progressively establishes a multi-layered, systematic information security protection framework.



In February 2018, Wistron achieved ISO/IEC 20000-1:2011 certification for its Information Service Management System. This certification reflects the Company’s commitment to delivering high-quality IT service management and complying with internationally recognized IT management standards, ensuring that its Information Technology Infrastructure Library (ITIL)-based operations meet expected performance standards. Wistron subsequently completed the transition to ISO/IEC 20000-1:2018 in January 2021, concurrently optimizing its information service management system and related processes to further strengthen IT governance capabilities and enhance overall service performance. The current certification, obtained in 2024, is valid until February 22, 2027.

- ISO/IEC 20000 changes the approach to implementing internal or outsourced IT services. Implementation Benefits:
- Achieved international best practices in IT management
 - IT service delivery is aligned with business objectives
 - Integration of personnel, processes, and technologies to support company objectives
 - Utilization of control measures for evaluation and maintenance of consistent service quality
 - Compatibility between ISO/IEC 20000 and the Information Technology Infrastructure Library (ITIL) facilitates continuous improvement efforts



In August 2017, Wistron achieved certification for the ISO/IEC 27001:2013 Information Security Management System, adopting the Plan-Do-Check-Act (PDCA) management model in accordance with the standard. The Company conducts at least one internal audit and one external third-party audit annually, and undergoes recertification every three years to ensure the continued effectiveness of its information security management mechanisms—demonstrating a long-term commitment to information security. In 2024, Wistron successfully obtained SGS certification and fully updated its certification to ISO/IEC 27001:2022. The certificate is valid until August 22, 2026.

- Wistron’s headquarters (located in the Neihu and Hsichi office areas), the Hsinchu plant, and all overseas manufacturing plants have obtained ISO/IEC 27001:2013 verification for critical infrastructure and essential information systems necessary for continuous operations. In 2022, all manufacturing plants achieved ISO/IEC 27001:2013 certification, covering 100% of the facilities.
- In August 2024, Wistron’s headquarters (Neihu and Hsichi offices), Hsinchu site, and all overseas manufacturing sites completed the full transition to the ISO/IEC 27001:2022 certification. Coverage rate reached 100%.

Note: Sites sharing a data center do not have independent certification.

Information Security Policy, Responsible AI (RAI) Systems Policy and Organization

To implement and uphold governance over information security and AI, Wistron ensures that critical information assets are managed with confidentiality, integrity, and availability in mind, and that AI systems operate in a compliant, secure, and reliable manner. These measures aim to meet applicable regulatory requirements and achieve RAI practices, thereby gaining customer trust, fulfilling commitments to shareholders, and ensuring the continuous operation of key business functions for sustainable management.

To strengthen the Company’s long-term competitiveness and enhance information security governance, Wistron’s Board of Directors approved the renaming of the Sustainability Committee to the ESG and Information Security Committee on April 2, 2025. Under this committee, an Information Security Executive Committee was established, led by the President & CEO and the Chief Digital & Information Security Officer as its highest-level executive sponsors, demonstrating the Company’s commitment to both information security and Responsible Artificial Intelligence (RAI). The committee oversees the implementation of the Company’s information security and RAI governance frameworks, technical standards, and operational practices. Wistron appointed the Chief Information Officer (CIO) as the Management Representative and the Head of the Information Security Governance Division as the Executive Secretary to coordinate the Company’s information security and RAI initiatives. Wistron has established an Information Security Policy and a Responsible Artificial Intelligence Systems Policy as the foundation for its management framework, protecting the information assets of employees, customers, suppliers, and business operations while supporting the Company’s sustainable development.

Information Security Policy

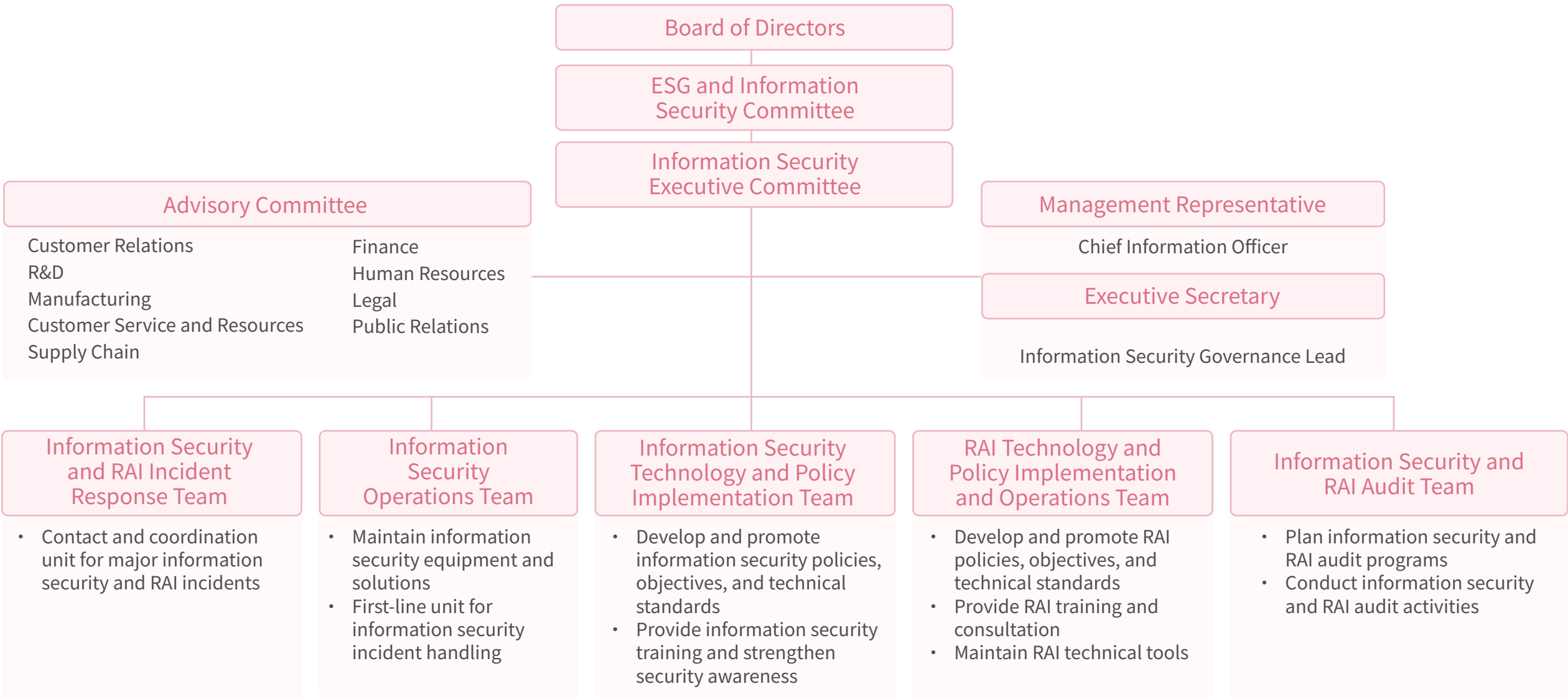
To protect information related to Wistron’s products and services, prevent unauthorized access, modification, use, or disclosure, mitigate losses caused by natural disasters, and ensure the timely availability of complete and usable information, the Company is committed to information security management. This commitment is intended to safeguard the confidentiality, integrity, and availability of the Company’s critical information assets, comply with applicable laws and regulations, earn customer trust, fulfill commitments to shareholders, and ensure the continuity of critical business operations. For further details, please refer to Wistron’s [Information Security Policy](#).

Responsible AI (RAI) Systems Policy

To ensure Wistron’s AI products and services and address the opportunities and challenges presented by AI, the Company has established a RAI Systems Policy to govern core RAI principles such as security, equity, stability, and reliability through the AI life cycle of planning, design, development, testing, and deployment. Wistron ensures compliance with related regulations and, thereby, secures customer trust, fulfills its commitment to shareholders, and supports Wistron’s sustainability, guaranteeing the operations of important company functions. For details, please refer to the [Responsible AI Systems Policy](#)

Information Security Executive Committee Structure

The Information Security Executive Committee convenes on a quarterly basis. Ad hoc meetings may be convened when necessary, and members of the teams are required to attend. The meeting agenda includes information security and RAI incident reports, the report from each team on the implementation of their affairs, issues that require the cooperation of different units, other related suggestions, and extemporaneous motions. The Information Security Committee held four meetings in 2025, and the Management Representative reported to the Board of Directors in December on the implementation status of information security and RAI initiatives.

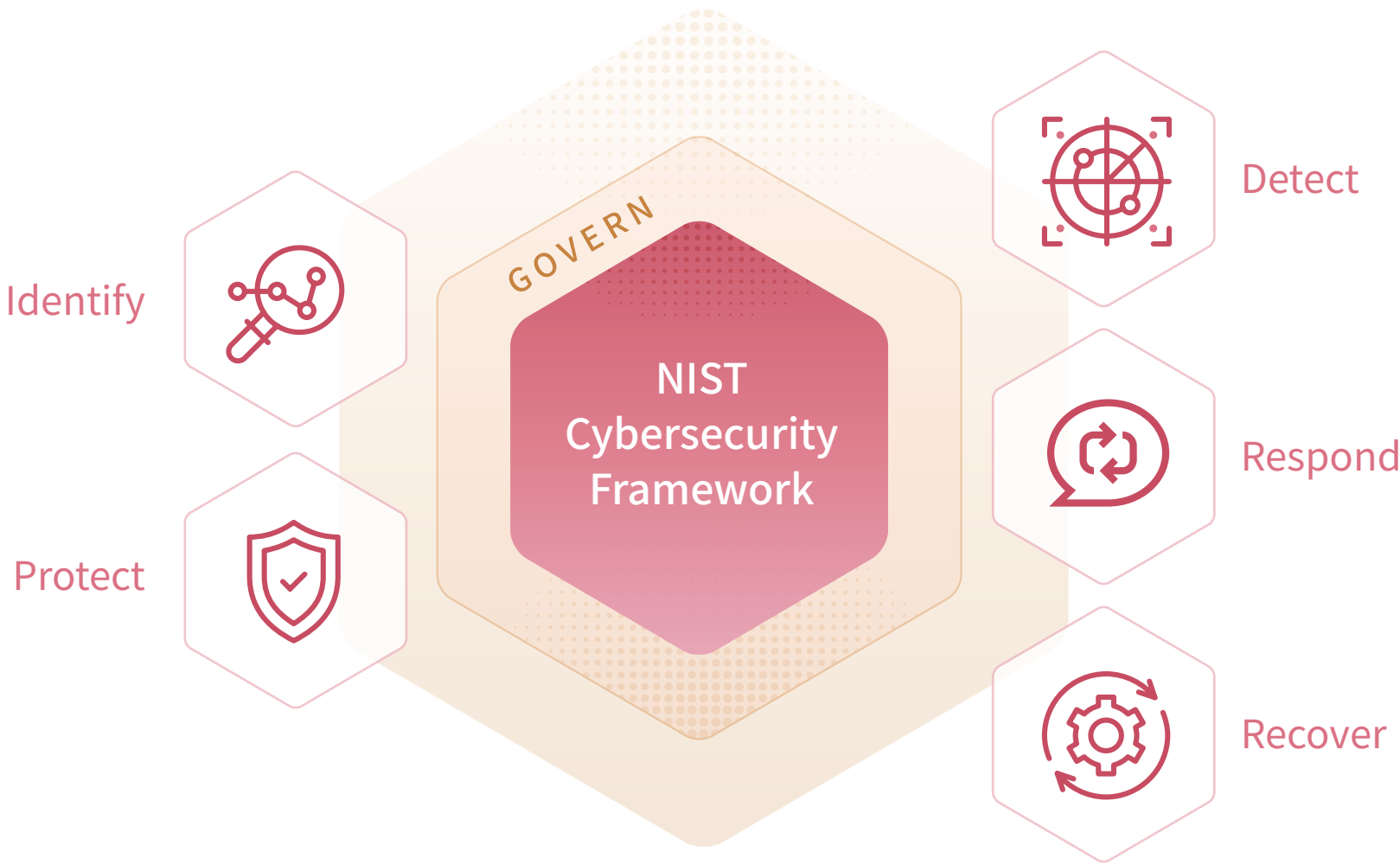


Information Security Management Strategies

To address information security risks arising from the rapidly evolving internal and external environments, Wistron has established a dedicated information security organization responsible for the planning and implementation of information security policies, as well as cybersecurity risk management. Through its overall governance framework, the Company systematically reviews and strengthens its information security management practices to enhance its ability to respond to cybersecurity threats and improve organizational resilience.

Wistron’s information security management encompasses three key domains: information technology security, operational technology security, and cloud security. Through the establishment and continuous enhancement of comprehensive internal information security management mechanisms, the Company strengthens system protection, data security, and operational stability, thereby reducing the potential impact of cybersecurity incidents on business operations. At the same time, the Company actively participates in cybersecurity intelligence-sharing platforms, including the High-Tech Cyber Security Alliance and the Taiwan Computer Emergency Response Team/Coordination Center (TWCERT/CC), to stay informed of security alerts, threat intelligence, and vulnerability information in a timely manner and proactively deploy protective measures. These efforts strengthen the Company’s overall cybersecurity capabilities and enhance the effectiveness of its risk management and control measures.

Wistron utilizes the Cybersecurity Framework (CSF) 2.0 stipulated by the National Institute of Standards and Technology (NIST) and its six core functions—Govern, Identify, Protect, Detect, Respond, and Recover—to assess overall cybersecurity maturity, develop its cybersecurity roadmap, prioritize initiatives, allocate resources, and implement continuous improvement plans. Information security/cybersecurity is based on the Zero Trust Architecture (ZTA), which requires that every user, device, and application must undergo identity authentication and obtain authorization before accessing network systems or assets. The scope of information security/cybersecurity protection will be further extended to cloud cybersecurity (including public cloud and private cloud) and operational technology (OT) cybersecurity. We will also introduce related cybersecurity standards and assessment models, such as Cybersecurity Capability Maturity Model (C2M2), CSA Consensus Assessments Initiative Questionnaire (CSA CAIQ), and ISO/IEC 62443. As such, we assure that our overall cloud cybersecurity and operational technology cybersecurity defense capabilities will be further strengthened in the future. In response to emerging risks associated with generative AI, Wistron continues to strengthen its AI governance framework by incorporating RAI principles and integrating them with existing cybersecurity governance structures and protection mechanisms. The Company is establishing a comprehensive governance system covering accountability frameworks, policy requirements, and automated monitoring mechanisms. Through ongoing training and practical implementation, Wistron continues to enhance organizational capabilities to support digital transformation while realizing its vision of innovation and sustainability, ultimately building a resilient, secure, and trustworthy enterprise environment.



Information Security/Cybersecurity Operation Measures

- Identify stakeholder groups associated with the information security/cybersecurity management system and regularly verify the needs of stakeholder groups for the information security management system (incl. customer demands for information security).
- Carry out social engineering drills and information security training for our employees to fully increase their information security awareness.
- Establish comprehensive and clear operating procedures to institutionalize the operations of the information security management system.
- Perform regular risk assessments to identify high-risk items and invest appropriate resources to reduce or transfer risks.
- Use tools and technologies to achieve timely and effective identification, defense, detection, adaptability, and recovery.
- Establish operating procedures for response and recovery in the event of information security/cybersecurity anomalies with the aim of rapid isolation of information security incidents, elimination of threats, and reduction of the scope and extent of impact.
- Perform regular disaster recovery exercises for key applications to ensure their effectiveness.
- Perform regular annual internal and external audits each year to review the entire management system and ensure normal operation and continuous improvement.
- Pay attention to new information security developments and technologies, and update defense or management practices to effectively block new forms of information security threats and reduce risks to operations.

Information Security Management Plan

Information Security Management and Audit Mechanisms

In order to protect the Company’s intellectual property (including confidential information) and confidential customer information, Wistron has conducted multiple self-assessments and external third-party audits annually since 2017. For self-evaluations, we follow the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 standards. For external third-party audits, we comply with ISO/IEC 27001 standards and our customers’ information security requirements. These audit activities aim to ensure the effectiveness and continuous improvement of information security measures, while also strengthening internal information protection mechanisms. To support business unit development and strengthen industrial control system (ICS) security, Wistron’s headquarters and Kunshan site have successfully obtained multiple international automotive cybersecurity certifications, including ISO/IEC 21434 and TISAX. These achievements demonstrate industry-leading automotive cybersecurity capabilities and further enhance the Company’s competitive advantage in automotive information security.

Wistron actively reinforces internal control mechanisms through self-assessments conducted by operational units, in conjunction with audits by the Information Security Governance Office and the Audit Department, as part of a three-line defense. This ensures the effective implementation and continuous improvement of information security measures across all sites.

In 2025, operating units conducted reviews of the computerized information systems cycle and its 11 sub-cycles through the Internal Control System (ICS) in July and December. The comprehensive self-assessment covered information systems and security policies, organizational design, and the effectiveness of control design and implementation. During the same period, the Information Security Governance Office conducted internal audits in accordance with the Information Security Internal Audit Management Procedures, reviewing the implementation and compliance status of information security policies and operating procedures across global operations. The audits were completed with no material non-conformities identified. In May, the Audit Office conducted a review in accordance with the “Internal Audit Implementation Guidelines,” focusing on information systems and security risks. The audit assessed the appropriateness of internal control systems, the implementation of general operating procedures, and specific audit projects. No major internal control deficiencies were found.

Since 2023, Wistron has received the Taiwan Corporate Sustainability Award (TCSA) Information Security Leadership Award for three consecutive years. In 2025, the Company also received the Automotive Cybersecurity Management Excellence Award from SGS Taiwan, demonstrating the Company’s exemplary role and leadership position in information security management across the industry.

Software Development Security

In order to control the security of the software development lifecycle (SDLC) and achieve “shift left” security to thereby reduce the operational costs associated with application security and maintenance, Wistron has adopted the DevSecOps (Development, Security, and Operations) mechanism. This approach enhances collaboration among the development, operations, and information security teams. Additionally, Wistron has adopted the DevSecOps Maturity Model (DOSMM) from the non-profit organization OWASP (Open Web Application Security Project) to assess the overall maturity of software development practices. This ensures that the software released meets predefined information security maturity standards. Furthermore, the incorporation of Software Composition Analysis (SCA) technology into the development workflow enhances the security quality of the software.

Data Protection Policy

In accordance with its Data Protection Policy, Wistron is comprehensively strengthening control over governance, technologies, and processes. The Policy covers both confidential business information and personal data. For confidential business information, Wistron applies classification management, strict access controls, encryption, and Non-Disclosure Agreement (NDA) requirements to prevent unauthorized disclosure of operational and technical information. For personal data, Wistron complies with GDPR, Taiwan’s Personal Data Protection Act, and applicable local regulations, conducting inventory management, minimizing data collection, limiting processing to specified purposes, and managing access permissions. Endpoint and gateway Data Loss Prevention (DLP) tools are deployed across email, endpoint devices, cloud services, and storage platforms to identify sensitive information and block high-risk activities. Through monitoring, audits, and key performance indicators, Wistron continues to enhance governance maturity.

Information Security Risk Management for the Supply Chain

In terms of supplier information security management, Wistron follows the Information Vendor Risk Management (VRM) process to classify and tier vendors, assessing their information security management life cycle from the perspectives of security, risk, and privacy. The life cycle covers the procurement phase (tier assessment, risk score assessment, contract), ongoing third-party risk management (risk score assessment and remediation), and the eventual offboarding.

A total of 306 vendors were identified in 2025. Vendors were classified into tiers based on risk factors such as the importance of the services they provide, their relevance to customers and revenue, and their ability to directly access the Company’s network environment and confidential information. Vendors are classified into three tiers, with Tier 1 and Tier 2 vendors—those with higher risk levels—required to meet Wistron’s information security assessment standards based on their respective levels of risk tolerance. Our risk score assessment identified 12 vendors that comply with Wistron’s information security standards.

Strengthen Information Security Awareness among Employees

To strengthen employee awareness of information security/cybersecurity, Wistron actively promotes cybersecurity education and training programs. Through a combination of online and in-person courses, the Company covers topics such as general information security awareness, the “Information Security/Cybersecurity Essentials” series, and phishing email identification and prevention, helping employees understand fundamental security concepts and practical applications. In 2025, a total of 19,702 training completions were recorded, amounting to 10,930 training hours. Additionally, disciplinary actions were taken for 43 incidents involving violations of information security policies, reinforcing the importance of information security.

To further enhance the professional capabilities of its cybersecurity team, Wistron encourages employees to participate in security conferences and related training programs. In 2025, 187 information security and secure software development personnel completed 5,050 hours of professional training. The training covered six core cybersecurity courses, five secure software development courses, and various international certification programs, including EC-Council CEH (Certified Ethical Hacker), CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor), and CompTIA certifications. These programs have not only strengthened the team’s technical expertise but also enhanced its ability to address a wide range of cybersecurity threats, thereby improving the Company’s overall defense capabilities. The implementation of this program aims to ensure that Wistron remains equipped to meet rapidly evolving cybersecurity challenges, safeguard its information assets, and increase employees’ awareness and responsiveness to information security/cybersecurity risks, maintaining a competitive advantage in the field.

Spotlight

TCM Information Security Professional Development Program

To enhance overall information security/cybersecurity management and respond to increasingly complex cybersecurity challenges, Wistron launched the Talent Competency Model (TCM) in 2021 to ensure that its cybersecurity personnel possess the necessary skills and knowledge. Based on workforce assessments, the program defines four key roles—Security Governance, Security Engineering, Security Analysis, and Secure Software Development—each with five competency levels. Annual capability assessments are conducted to inform targeted development and advancement plans, ensuring that talent continues to evolve in line with advancements in the cybersecurity field. By 2025, a total of 88 employees—including 28 dedicated cybersecurity personnel—had joined the program, demonstrating Wistron’s strong commitment and continued investment in cybersecurity talent development.



Social Engineering Drills

To educate employees on information security/cybersecurity, the Company provides e-Learning resources and holds social engineering exercises every six months on phishing email simulations, reviews of employee information security awareness, and information security education and training. In addition, the Company publishes cybersecurity e-newsletter every month to enhance our employees’ awareness and vigilance of cybersecurity. The e-newsletter covers latest cybersecurity trends and recent major cybersecurity events at home and abroad. To mitigate information security/cybersecurity risks and minimize its potential impacts, employee violations against our Information Security Policy will result in penalties according to the “Implementation Guidelines for Employee Rewards and Penalties” and be factored into their performance evaluations.

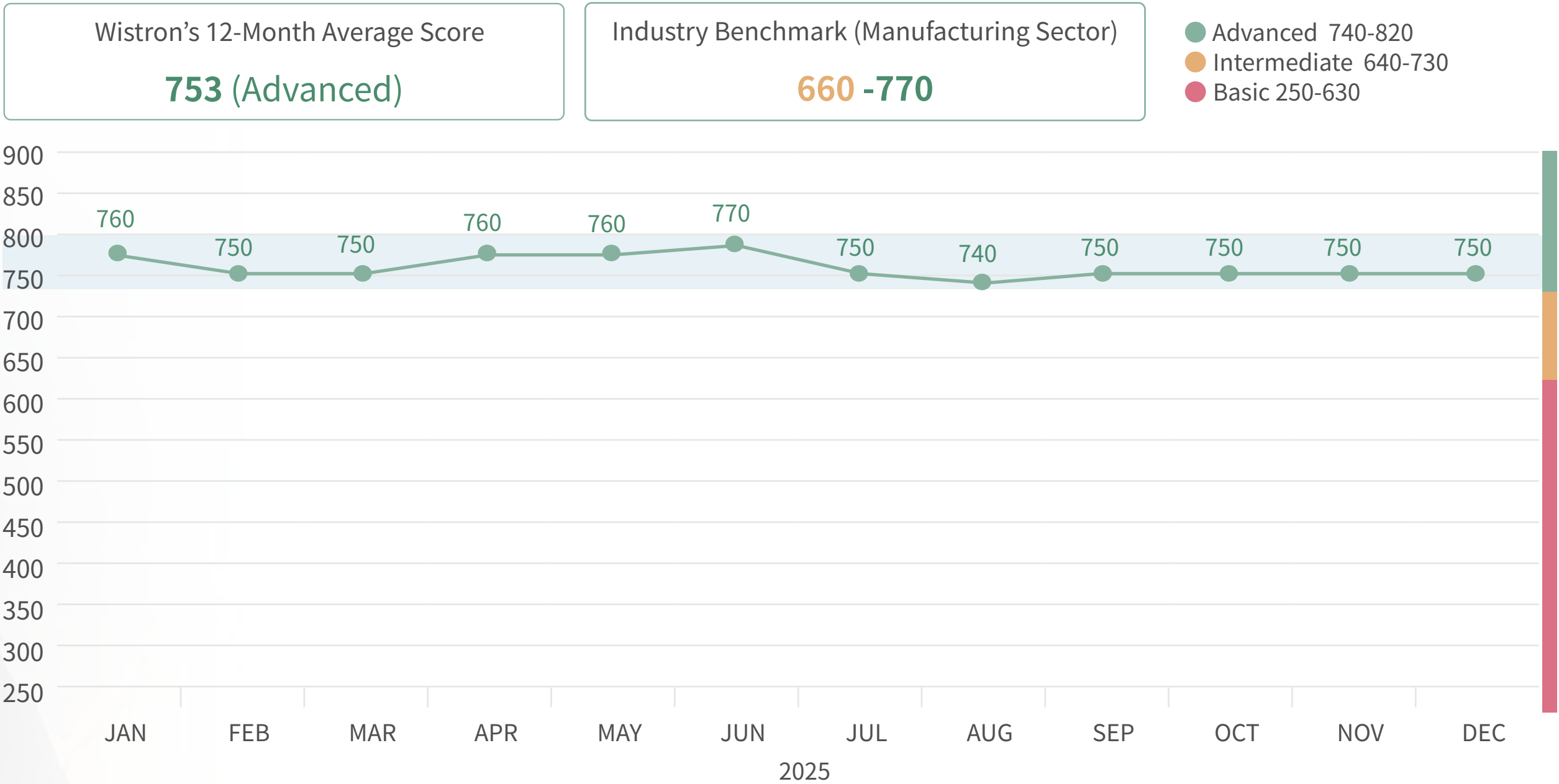
2022-2025 Phishing Click Rates from Social Engineering Drills at Wistron

Initiatives	Objectives		2022	2023	2024	2025
Social engineering drills every six months	<15% phishing click rate from social engineering drills	H1	9.3%	7.4%	7.8%	7.4%
		H2	10.2%	8.2%	12.6%	11.9%

Vulnerability Detection for Networks and Systems

Apart from monthly internal vulnerability scans, Wistron entrusts a third-party professional organization to conduct network and system penetration tests each year to protect Wistron’s corporate and personal information and prevent losses caused by leaks, theft, destruction, other human factors, or natural disasters. These tests reduce the impact of human factors or natural factors on the Company’s operations. The purpose of the tests is to understand and evaluate the status of the organization network environment and system security and verify the current information security protection safety rating and effectiveness to resolve vulnerabilities, improve operations, and strengthen system security. In 2021, we introduced red team drills, where external information security teams simulated attacks on the Company and attempted to achieve specified goals without affecting the Company’s operations. The red team drills allow us to comprehensively review our services and networks for any vulnerabilities and human errors in deployment. Moreover, we checked the integrity of identification, protection, detection, and response mechanisms from our information security maintenance and response team. In 2025, Wistron achieved an average score of 753 in its third-party cybersecurity assessment. Through external evaluations, the Company is able to promptly identify, address, and strengthen vulnerabilities in its networks and services.

2025 Wistron Corporation Third-Party Cybersecurity Assessment Results



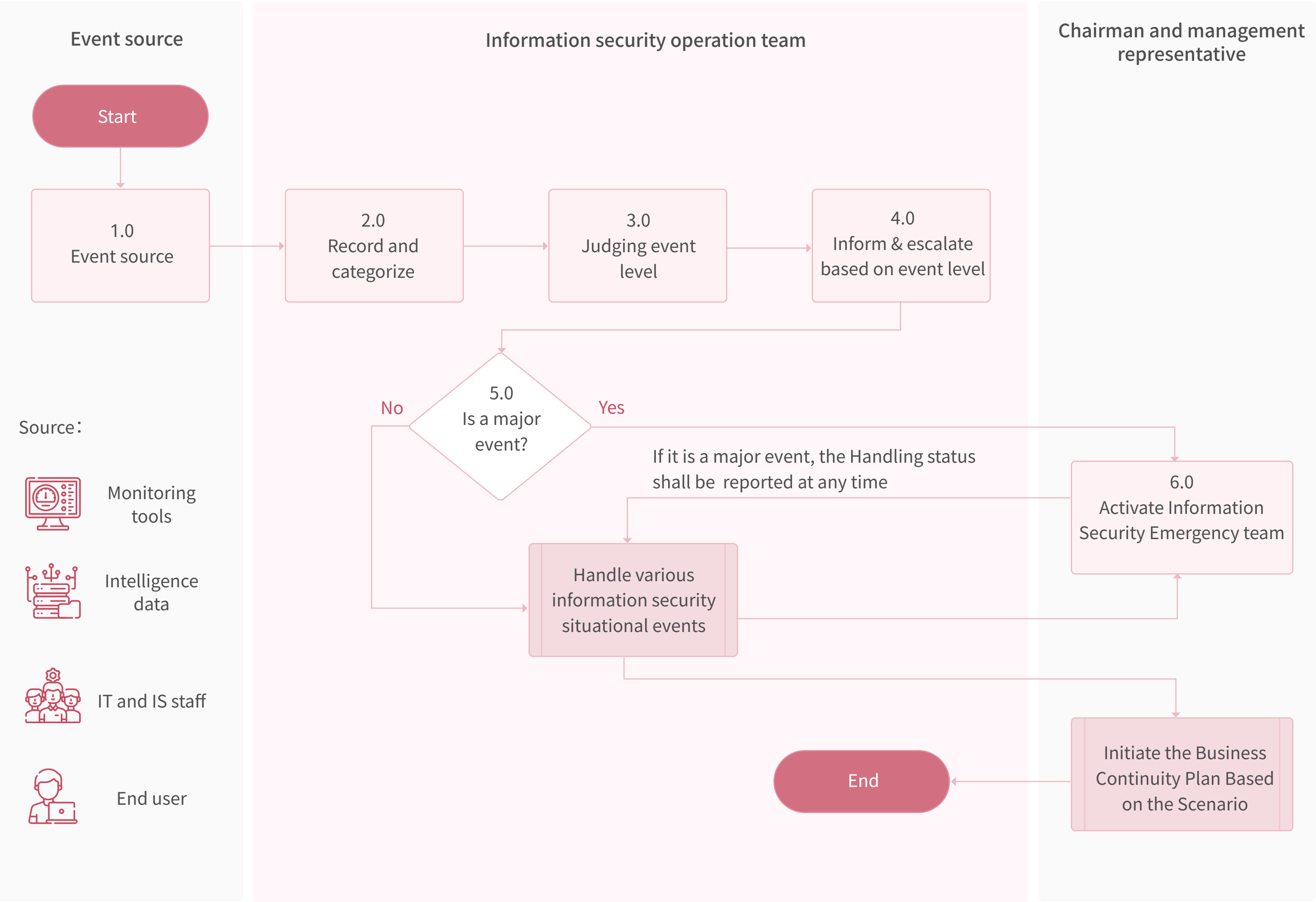
Information Security Alerts and Incident Management

To ensure the effectiveness of information security/cybersecurity management and enable prompt handling of security incidents, vulnerabilities, or suspicious activities, Wistron has established a comprehensive information security escalation process. This allows employees to immediately report issues and activate response mechanisms upon detection. Employees can report suspicious activities, vulnerabilities, or information security incidents to the appropriate personnel through various channels, including internal platforms such as the local IT Helpdesk, reporting systems, or by directly contacting the Information Security team. This process ensures that every security incident receives timely attention and appropriate response measures without delay.

To strengthen digital resilience and support sustainable operations, Wistron continues to enhance its information security governance framework by implementing the Advanced Persistent Threat (APT) system and maintaining round-the-clock cybersecurity protection through its Security Operations Center (SOC). The SOC integrates the expertise of internal information security professionals and external cybersecurity specialists to provide 24/7 real-time monitoring and threat detection, enabling comprehensive visibility into the Company’s cybersecurity posture. This approach facilitates the early identification of potential risks and minimizes the potential impact of cybersecurity incidents on operations, customers, and stakeholders.

With respect to information security incident management, Wistron has established a systematic and tiered response mechanism in accordance with its Information Security Incident Management Procedures. This structured process ensures that information security incidents are promptly addressed and effectively controlled. Through continuous feedback mechanisms, the Company further strengthens its protection capabilities and enhances organizational resilience against digital risks, thereby supporting operational stability and the achievement of its long-term sustainability objectives.

Information Security Event Management Process



Business Continuity Management and Disaster Recovery Drills

To ensure the continuity of operations and critical business functions while minimizing the impact of major disaster events on key information systems, Wistron has established a comprehensive Information Security Business Continuity Plan. This plan is designed to address various unexpected situations and ensure the rapid and effective recovery of critical application systems in the event of information security/cybersecurity incidents or natural disasters, thereby preventing operational disruptions. According to the plan, Wistron conducts at least one test every six months through tabletop exercises simulating the Business Continuity Plan or Cybersecurity Incident Response Plan. These drills simulate potential cyber threats or disaster scenarios to verify the feasibility of the response plan. Through these regular tests, Wistron is able to effectively identify potential vulnerabilities, enhance response capabilities, and reduce the risk of operational disruption. In addition to drills, Wistron conducts at least one annual backup data restoration test to verify the readability of backup data, the availability of storage media, and the feasibility of recovery procedures for critical assets. These tests ensure that all data can be successfully restored within the designated timeframe, thereby reducing system recovery time and safeguarding business continuity.

The global IT center also selected 27 backup storage media for seven key functional systems and databases in 2025. Recovery testing was successfully completed for the backup data. The annual global computer center disaster recovery drills revealed that the maximum tolerable data loss time during disasters (Recovery Point Objective, RPO) is 1.85 hours. After a disaster occurs, the maximum tolerable information service recovery time (Recovery Time Objective, RTO) is 20.50 hours. The results of the drills in the last four years have met the Company’s targets.

Strategy	Objectives	2022 Results	2023 Results	2024 Results	2025 Results
Annual disaster recovery simulations for key applications and systems to ensure continued operations and the uninterrupted provision of Company services.	RPO of SC2 Services ≤ 4 hours	0.9 hours	1.0 hours	0.6 hours	1.85 hours
	RTO of SC2 Services ≤ 24 hours	18.83 hours	22.11 hours	19.22 hours	20.50 hours

Note:
1. RPO: Recovery Point Objective (maximum tolerable data loss time in the event of a disaster)
2. RTO: Recovery Time Objective (maximum tolerable time to restore information services after a disaster)

Mitigate Information Security Risks with Information Security Insurance

In 2021, Wistron purchased global information security insurance policies as a group. Apart from mitigating risks, we also hope to further receive the help and resources of external information security experts through the international insurance market, leveraging their preventative solutions to strengthen existing information security/cybersecurity measures so that we may respond to growing information security threats and achieve corporate sustainable management.

Information Security Incidents in Past Four Years

From 2022 to 2025, with the exception of two material information security incidents in 2024, the Company did not experience any incidents involving the leakage of confidential information that affected the personal data of customers or employees, nor did it incur any related regulatory fines or penalties. In 2024, Wistron experienced two major information security incidents. The first occurred on March 25, when a fire at the Hsinchu site in Taiwan caused a server room power outage. The second occurred on October 4, when the Company’s official website was subjected to a Distributed Denial-of-Service (DDoS) attack. In both cases, relevant defense mechanisms were immediately activated. There were no significant impacts on Company operations, and no personal data or internal documents were compromised.

Number of information security violations and fines/year	2022	2023	2024	2025
Information security or network security violations (no. of cases)	0	0	2	0
Data leak incidents (no. of cases)	0	0	0	0
Information security violations that involve customer information (no. of cases)	0	0	0	0
Number of customers and employees affected by the data leak	0	0	0	0
Amount of fines for information security/cybersecurity or network security related incidents (NTD)	0	0	0	0

Privacy Protection

To implement personal data protection and management, Wistron formulated its [Privacy Policy](#) with reference to the laws and regulations of the jurisdictions in which it operates, and in alignment with the relevant requirements of the European Union’s General Data Protection Regulation (GDPR) as the highest guiding principle for privacy protection. The Policy applies to all Wistron personnel, subsidiaries, and joint ventures over which Wistron has significant influence, as well as suppliers, contractors, external consultants, and other third-party partners. The Policy outlines clear specifications and requirements for the use and protection of personal data, as well as related matters. All internal personnel and third-party partners are required to strictly adhere to the Policy to ensure the security of personal data and protect the rights and interests of relevant stakeholders.

Wistron incorporates privacy and personal data protection into its Enterprise Risk Management system and promotes related management actions in accordance with the [Risk Management Policy and Procedure](#) to reduce operational risks and potential impacts. In addition, the internal control department conducts an internal audit project every six months through the Internal Control System (ICS) to review the collection, processing, and transfer of personal data, ensuring that all operations comply with local regulations and internal Code of Conduct.

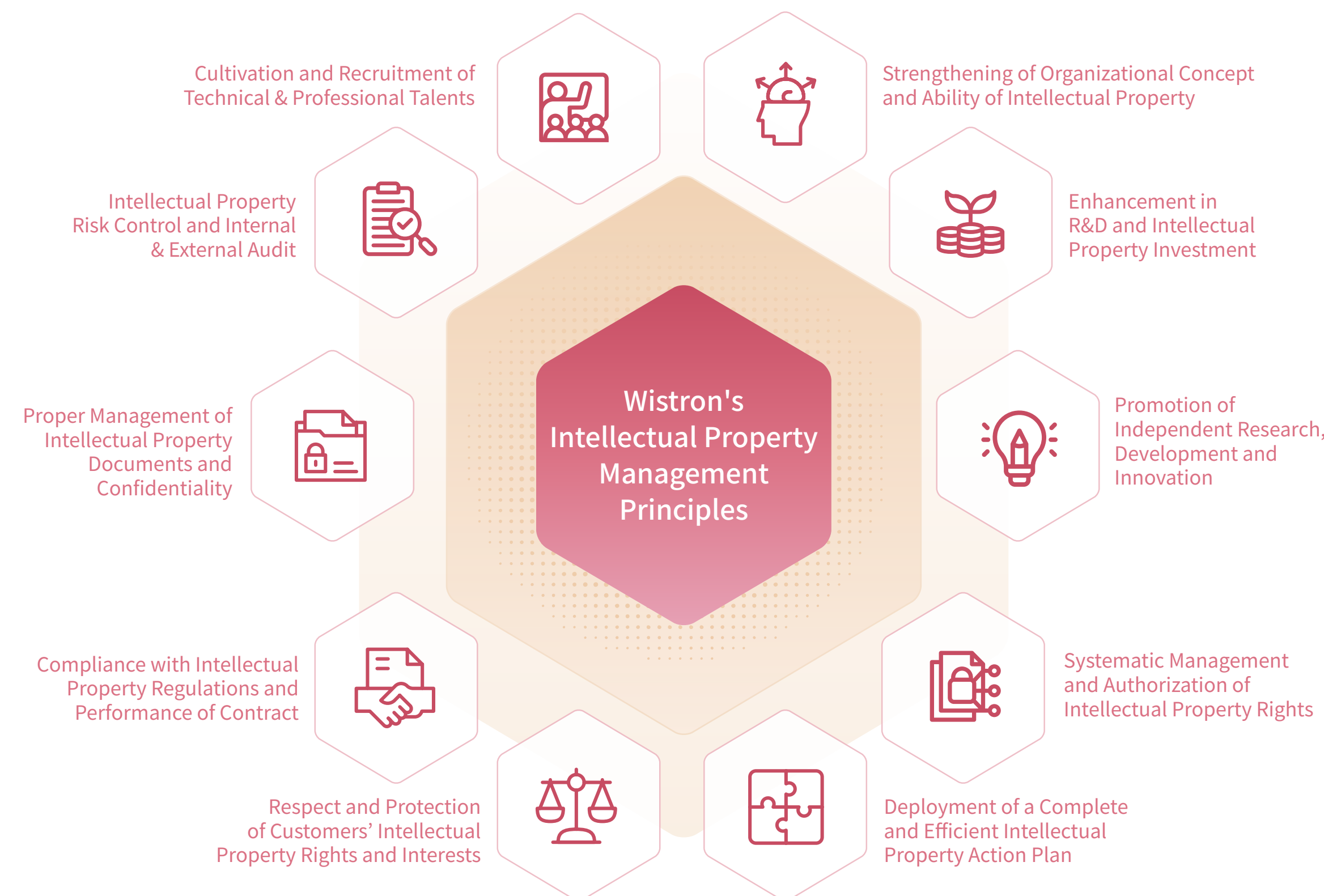
Wistron has established complaint channels for privacy-related incidents. If anyone discovers or suspects a violation of privacy rights or a breach of the Policy, they may report the issue through the Privacy Protection Hotline at (02) 6616-9999 ext. 25740 or via email at ethic@wistron.com. We adopt a zero-tolerance policy toward privacy violations. Any individual found in breach of this Policy will be subject to disciplinary action in accordance with the relevant provisions of the [Code of Conduct](#), ensuring the rigor of personal data management procedures.

To strengthen privacy awareness, Wistron promotes its Privacy Policy and emphasizes its importance across global operating sites through internal electronic bulletin boards, emails, physical notices, and other communication channels. In addition, since 2024, Wistron has provided the “Privacy and Data Protection Awareness” training to all employees across 31 global operating sites in nine languages. In 2025, a total of 18,389 employees completed the training, achieving a 100% coverage rate and further strengthening employee awareness of and compliance with personal data management practices.

“Strictly guarding customer confidentiality and upholding the principle of integrity” is Wistron’s core commitment to customer privacy. We strictly adhere to our Privacy Policy and ensure that customer data is never used for secondary purposes (0%), safeguarding the confidentiality of all information. From 2022 to 2025, Wistron has not received any privacy-related complaints or penalties from regulatory authorities or external parties, demonstrating our rigorous management and consistent implementation of personal data protection practices.

5.2.3 Intellectual Property

Wistron places strong emphasis on the management of intellectual capital. Through its comprehensive intellectual property management policy, the Company strengthens its R&D capabilities, promotes high-value-added innovative products and technical services, and enhances manufacturing efficiency and quality. These efforts enable Wistron to build a forward-looking intellectual property portfolio (IP Portfolio) that further strengthens its competitive advantage. In the future, Wistron will continue to implement its consistent intellectual capital management plan by aligning it with the Company’s strategic considerations and operation objective of “Sustainability through Innovation” to ensure the timely creation, effective management, and flexible utilization of intellectual property rights.



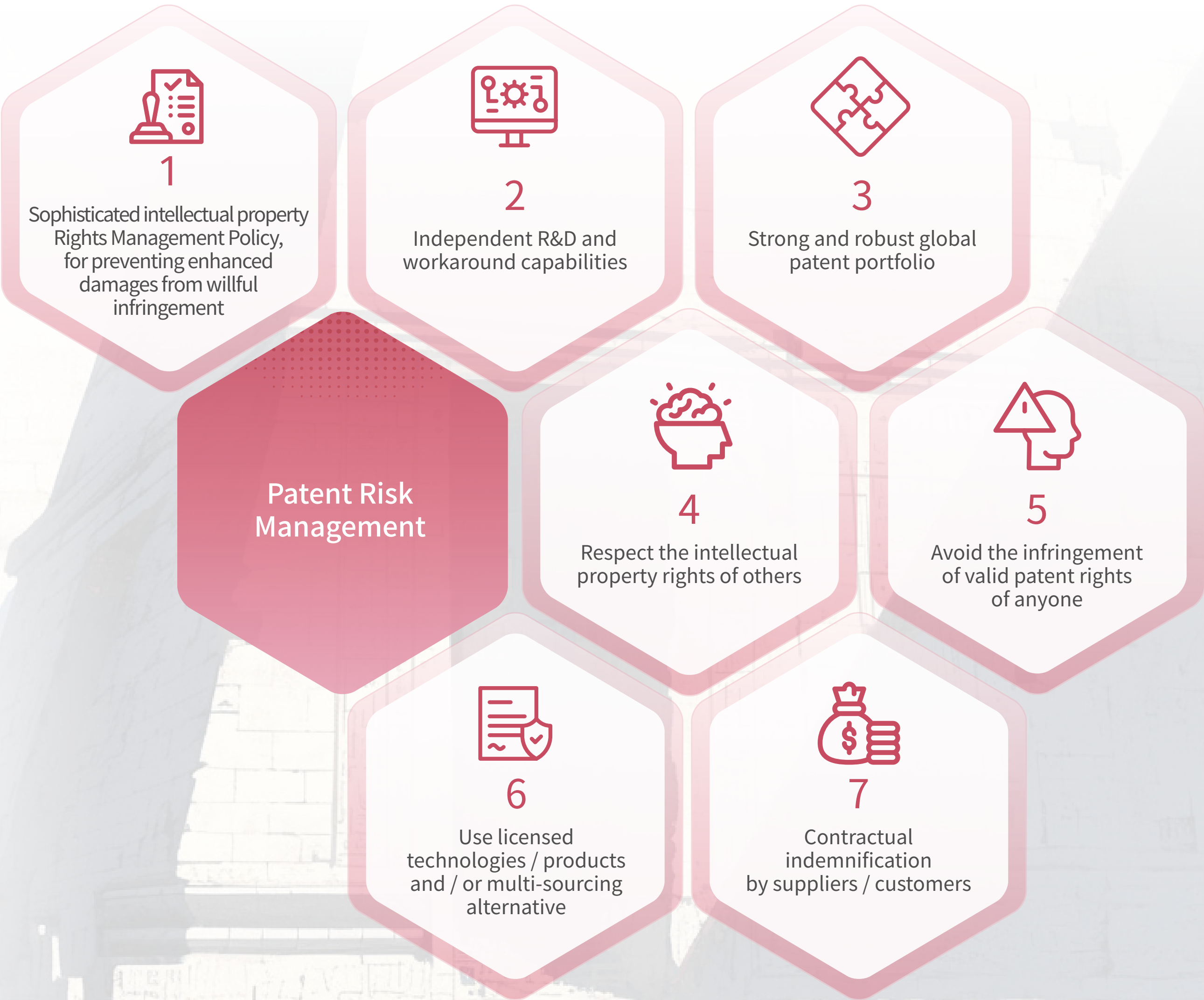
Patent Portfolio Management

Wistron is committed to building a robust and efficient global patent portfolio. Through a clearly defined patent strategy, the Company ensures that its technological achievements are fully protected while safeguarding the interests of its customers. To date, Wistron holds over 6,500 multinational patents. This strong patent portfolio enhances technological competitiveness and secures a market advantage for its innovations.

In terms of patent management, Wistron integrates its overall corporate strategy and business development objectives to actively drive innovation and patent deployment, ensuring the maximization of patent value. The patent team works closely with the R&D departments through brainstorming sessions, patent big data analysis, and proposal review mechanisms to identify high-quality ideas and generate goal-oriented invention proposals. Additionally, the team applies over 300 evaluation criteria to rigorously review patent specifications, ensuring that every patent meets high-quality standards. The end-to-end process—from invention proposal, patent search, claim scope design, drafting and translation, filing strategy, and response, to post-grant maintenance and management—is designed to ensure that Wistron’s patent assets maintain long-term competitive advantages.

To strengthen the professional capabilities and patent knowledge of patent professionals, Wistron has strengthened internal training, offering the Patent Classroom among other professional courses. Over 1,323 participants completed and passed tests for courses launched in 2025, with total hours amounting to around 700 hours, confirming that Wistron has developed a systematic learning mechanism. Wistron has established an incentive system for inventive contributions. Through a reward and public recognition mechanism, it motivates employees to actively engage in innovation, further enhancing the quality and market competitiveness of Wistron’s products and technical services.

In terms of patent quantity and quality management, Wistron continues to pursue independent innovation and patent development, while also engaging in patent acquisition, investment, expiration-related cancellations, divestitures, and selective non-maintenance to optimize the patent portfolio. With a consistent evaluation framework, Wistron maintains comprehensive oversight of patent coverage, quality, and market value. The Company also uses benchmarking metrics provided by third-party assessment institutions to compare its portfolio with competitors and industry leaders, further enhancing patent competitiveness and maximizing the commercial value of its patent portfolio.



Trademark Management

Trademarks are a vital representation of Wistron’s products and services. A well-planned trademark strategy reinforces the Company’s brand image and ensures long-term brand resilience. Wistron currently holds registered trademarks in 37 major countries across five continents, establishing a comprehensive global trademark presence.

Sustaining a brand is a direct reflection of a company’s commitment to long-term corporate sustainability. To effectively manage its trademarks, Wistron has established a dedicated trademark team, which works directly with international law firms to manage trademark affairs. This approach helps control trademark-related costs and provides timely access to first-hand information across different jurisdictions. The Company’s current trademark management priorities include:

- 1. Apply for trademark registration in alignment with business development plans and systematically deploy trademark portfolios.
- 2. Conduct trademark clearance searches before any public use to avoid infringement of others’ trademark rights.
- 3. Monitor trademarks globally to prevent counterfeiting or unauthorized use of Wistron’s brand.
- 4. Evaluate the current usage of trademarks and exclude those that no longer provide economic value.

Through a rigorous and systematic trademark management framework, Wistron has not faced any trademark infringement disputes since its establishment. To further strengthen its trademark management system, Wistron officially adopted the credible Taiwan Intellectual Property Management System (TIPS) in 2023, with certification valid through December 31, 2026.

Protection of Trade Secrets and Confidential Information

Trade secrets and confidential information are important intellectual assets for Wistron. We use various control mechanisms to ensure the protection of trade secrets and confidential information. Apart from maintaining our competitive advantage, these protected assets can drive innovation and ensure our customers’ rights. No substantiated complaints concerning the loss of customer data in 2025.

To protect confidential information of both Wistron and its customers, the Company utilizes cloud-based digital tools—such as encryption mechanisms, identity authentication, and access authorization features within Microsoft Office 365—to safeguard sensitive corporate documents. Meanwhile, we require confidential information and trade secret protection training for all new employees to ensure that employees fulfill our confidentiality commitments to our customers.

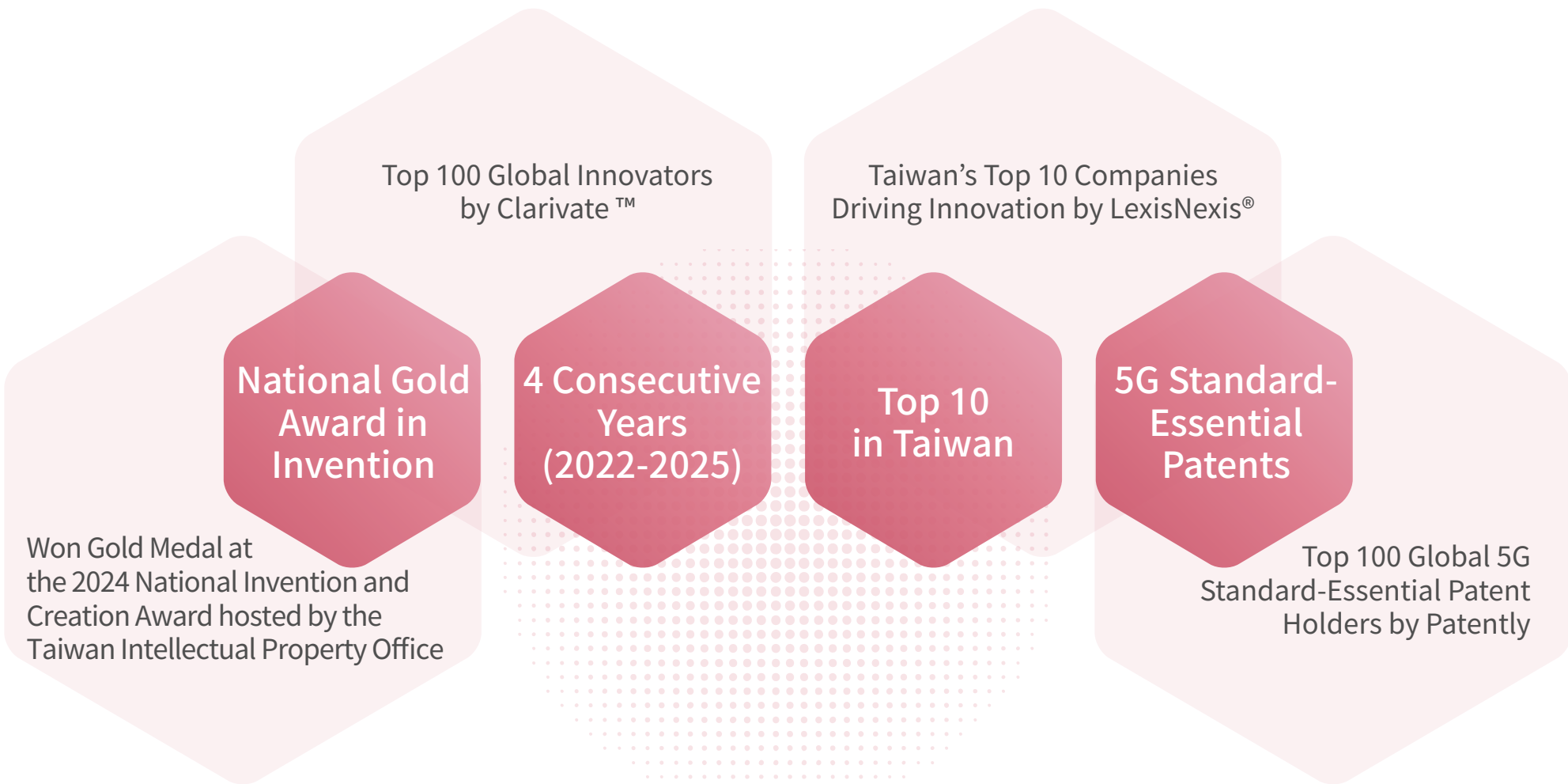
We have signed confidentiality agreements with our customers and related suppliers, requiring both parties to protect confidential information. Over the past five years, customer information has been handled exclusively by designated departments. Specific procedures are in place for contract execution and document access, and archive rooms are equipped with access control and surveillance systems, thereby reducing the risk of improper disclosure and information leakage. We have also joined the Taiwan Association for Trade Secrets Protection to continue tracking changes to related laws and the industry.

Status of Intellectual Property Risk Management Policy Implementation

Since 2020, Wistron has implemented its Intellectual Property Rights Management Policy. The key implementation actions in 2025 are outlined below and were reported to the Board of Directors on December 19, 2025:

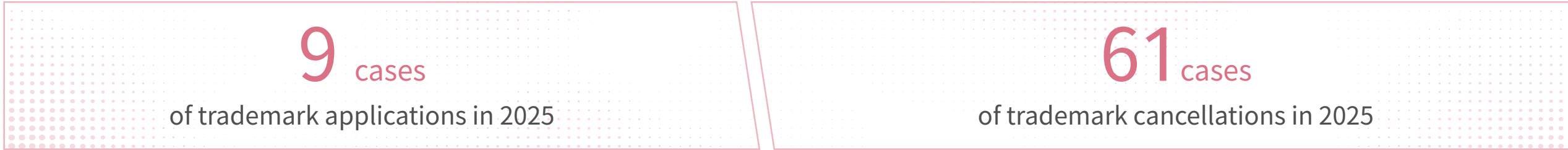
Global Patent Portfolio Optimization and Greater Competitiveness

Wistron continues to focus on enhancing technology quality and patent value. Each year, the Company conducts a comprehensive evaluation of its existing patent assets, eliminating outdated or lower-value patents (including expirations, cancellations, sales, or selective non-maintenance). At the same time, Wistron actively revitalizes its patent portfolio by participating in domestic and international patent programs and filing strategically valuable patent families. Currently, according to comprehensive indicators, Wistron’s comprehensive patent portfolio rank among the industry leaders and has steadily improved to surpass those of leading international enterprises. Key achievements in 2025 are as follows:



Global Trademark Monitoring and Portfolio Optimization

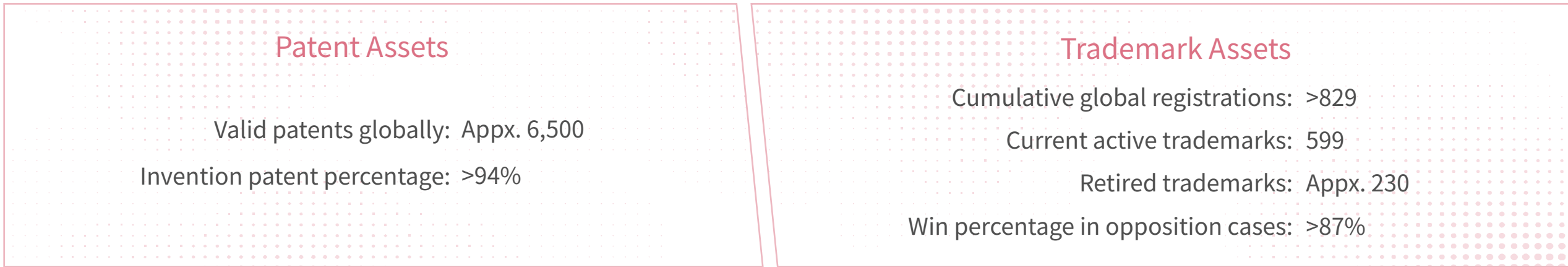
Wistron has always attached great importance to protecting its own intellectual property rights while respecting the intellectual property rights of others. Before any trademark is officially used externally, a clearance process is conducted to assess the risk of potential infringement. In addition, Wistron utilizes a global trademark monitoring system to track the use and applications of trademarks by others across various countries, helping to prevent counterfeiting and unauthorized association. In 2023, the Company obtained certification under the Taiwan Intellectual Property Management System (TIPS), which is valid for a three-year period (2024–2026). For expired trademarks, the Company evaluates the need for renewal based on actual business conditions and excludes those that no longer provide economic value. In 2025, no third-party applications for identical or confusingly similar trademarks were identified; therefore, no trademark oppositions were initiated during the year.



Protection of Trade Secrets and Confidential Information

To safeguard the Company’s and customers’ confidential information, Wistron has obtained ISO/IEC 27001 Information Security Management System certification and implemented comprehensive management measures across policy, technology, and personnel levels:

- Conduct social engineering simulation exercises every six months to enhance employees’ awareness of phishing
- New employees are required to complete training on confidential information and trade secret protection
- Leverage encryption mechanisms, identity authentication, and access authorization features within Microsoft Office 365 to safeguard sensitive corporate documents
- Regularly perform software audits using System Center Configuration Manager (SCCM) to ensure license compliance
- Confidentiality agreements are signed with all customers and suppliers, requiring mutual protection of confidential information



To enhance the Company’s brand image and brand trust, Wistron has established the following intellectual property management policies and objectives:



5.3 Moving Toward a Sustainable Supply Chain

Suppliers are key partners in Wistron’s operational and sustainability efforts. We regard the supply chain not only as an integral part of business operations but also as a critical driver for achieving our sustainability goals. Accordingly, Wistron has designated sustainable and responsible procurement as one of its Six Sustainability Strategies (ESG 6-Pillar), fully integrating it into procurement decision-making and management processes. Guided by risk management, competitive advantage, and cost optimization, we systematically steer suppliers to continuously enhance their performance across environmental, social, and governance (ESG) dimensions in accordance with the ISO 20400 sustainable procurement principles and the Responsible Business Alliance (RBA) Code of Conduct. Since 2024, Wistron has embedded the aforementioned international standards and sustainability principles into its procurement policies and strategies. Centered on the six core subjects of social responsibility—organizational governance, human rights, labor practices, fair operating practices, consumer issues, and environmental protection—Wistron promotes the implementation of its sustainability goals through a systematic supplier management process and cross-functional collaboration. From 2025, Wistron has actively promoted the adoption of UL2799 Zero Waste to Landfill (ZWTL) practices among suppliers. This initiative reduces waste generation, enhances recycling and reuse, and minimizes the environmental impacts of incineration or landfill disposal, thereby improving the overall environmental performance and sustainability resilience of the supply chain.



5.3.1 Supply Chain Management Framework and Overview

Sustainable Supply Chain Strategy

Wistron values collaboration and mutual growth with its suppliers. Building on its Sustainable Procurement Policy and in response to customer expectations, Wistron has developed a comprehensive sustainable supply chain strategy. This strategy focuses on optimizing the core competitiveness of strategic suppliers, deepening regional strategic collaboration, and strengthening supply chain resilience. By implementing these strategies, Wistron enhances suppliers’ competitiveness in terms of technology, resources, and market adaptability. Regional cooperation further increases the supply chain’s agility and efficiency, ultimately enabling the establishment of a more stable, flexible, and resilient sustainable supply chain system in an increasingly dynamic global market environment.

Sustainable Supply Chain Strategy



Governance Structure

Sustainable Supply Chain Management Organization

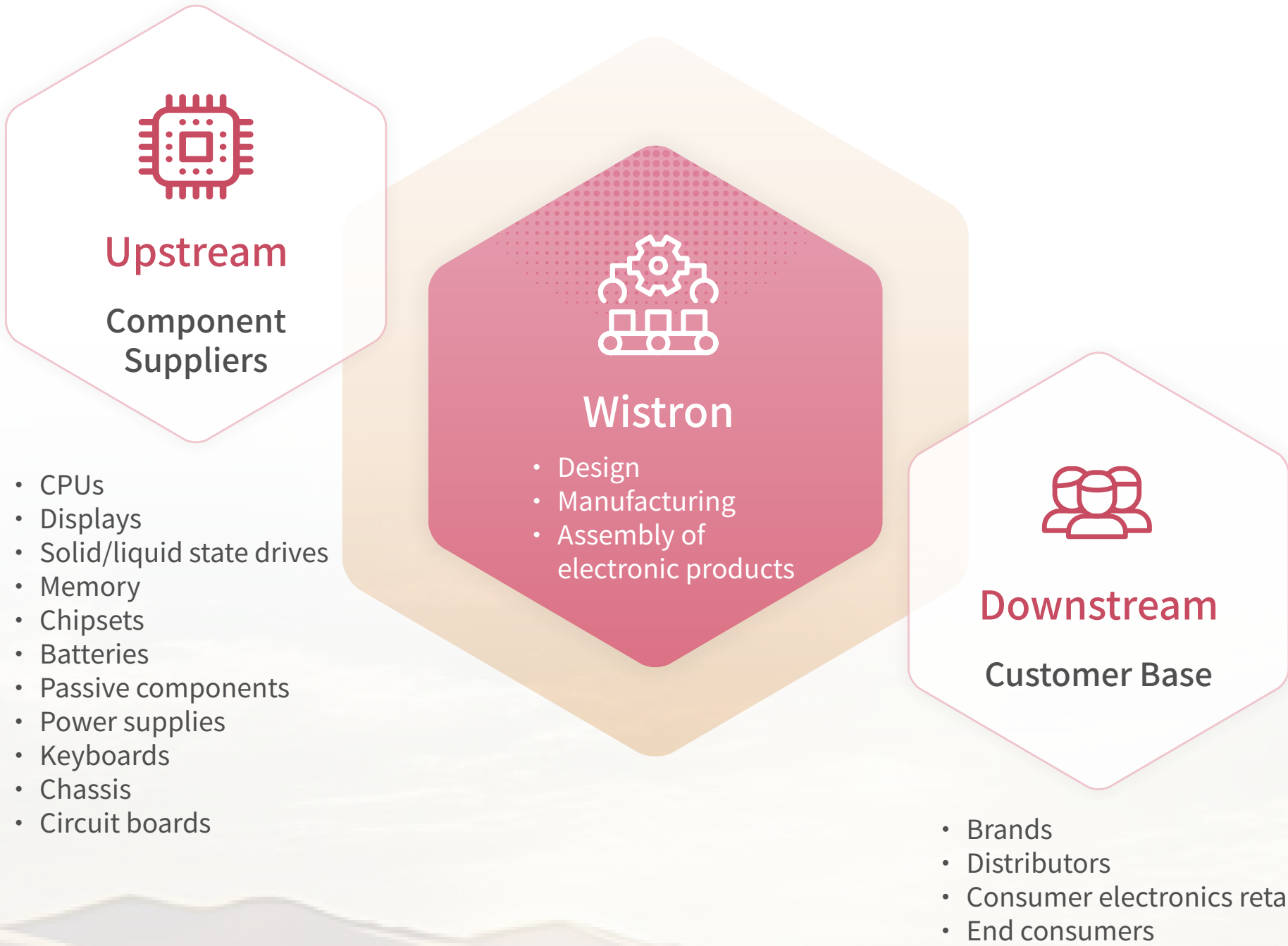
To ensure the comprehensiveness and effectiveness of sustainable supply chain management, Wistron designates the Board of Directors as the highest decision-making body for sustainable supply chain governance. The Board regularly oversees the progress and outcomes of various sustainability initiatives to ensure that all decisions and actions align with the Company’s long-term development goals. Through its functional committee—ESG and Information Security Committee—the Board reviews the work of the Sustainable Supply Base (one of the ESG 6-pillar strategies) twice a year to ensure the proper implementation of all sustainable supply chain management systems. In addition, the ESG Executive Committee tracks the execution progress and performance outcomes of each sustainable supply chain project on a monthly basis.



Wistron Value Chain

Wistron is a leading company in the global ICT (Information and Communications Technology) industry, with a long-standing focus on the design, manufacturing, and assembly of electronic products. Positioned centrally within the overall industry value chain, Wistron connects upstream suppliers of diverse components and critical materials with downstream international brands and end customers, establishing a highly integrated and stable framework for industry cooperation.

By continuously monitoring market trends and customer technology requirements, Wistron effectively integrates upstream and downstream resources, promotes cross-domain and cross-process collaboration, and further enhances overall supply chain efficiency, while strengthening product R&D, manufacturing flexibility, and market responsiveness.



Supply Chain Overview

As a key supplier of information technology products to the global market, Taiwan plays a vital role in the ICT industry. Rooted in Taiwan with a global outlook, Wistron leverages its strong technical capabilities to provide customers with comprehensive hardware and software solutions, along with one-stop system integration services. Wistron’s main suppliers fall into four major categories: electronic parts, mechanical parts, maintenance repair operation (MRO), and logistics suppliers. In 2025, Wistron engaged in transactions with 1,617 suppliers. To enhance management efficiency and strengthen collaboration with key partners, suppliers are categorized into tiers, enabling more focused and in-depth supplier management.

2025 Supplier Distribution by County/Region

	Total Number of Suppliers	Percentage of Purchase Amount (%)
Taiwan	513	58.54
China	859	31.96
Asia Pacific	134	4.39
Americas	73	3.42
Europe	22	0.19
Others	16	1.50
Total	1,617	100

With ongoing supply chain restructuring and adjustments to Wistron’s manufacturing sites, the supply chain has been reconfigured to ensure greater flexibility, reduce risks, and enhance supply chain stability. Tier 1 suppliers are those who have conducted more than six transactions per year and accounted for over 90% of the annual transaction amount. In 2025, there were 421 tier 1 suppliers. Based on transaction share and strategic importance, 232 of these were further identified as significant tier 1 suppliers¹.

Note :

1. Significant tier 1 suppliers: Including critical suppliers – high percentage of turnover (top 80% of annual transaction amount); ability of technology pioneering; the only source of supply is irreplaceable; high-risk suppliers - SAQ score below 80.
2. Significant non-tier 1 suppliers: (1) Agency transaction with SAQ score below 80 (Potentially high-risk suppliers); (2) The upstream supplier of the customer's designated trading supplier.

2025 Tier 1 Suppliers by Category

	Total Number of Suppliers	Percentage of Purchase Amount (%)
Electronic parts	168	59.06
Mechanical parts	200	35.76
Maintenance, Repair, and Operation (MRO)	39	2.92
Logistics	14	2.26
Total	421	100

2025 Suppliers by Classification

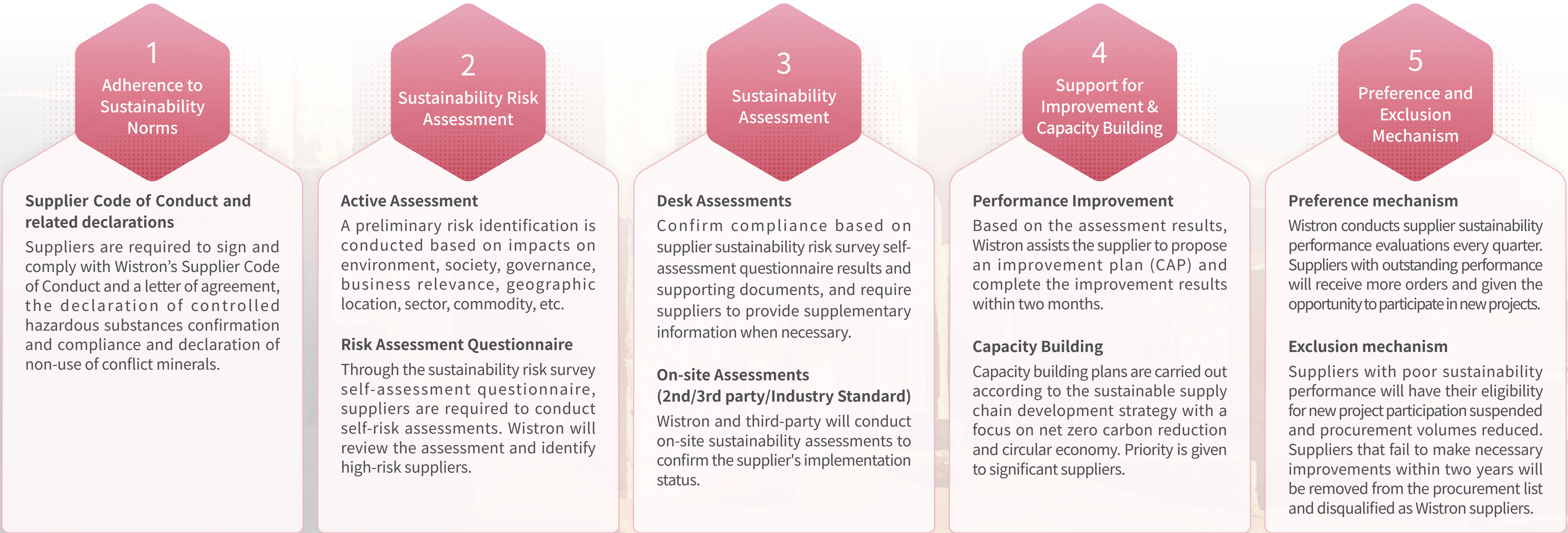
	Total Number of Suppliers	Percentage of Purchase Amount (%)
Tier 1 suppliers	421	95.40
Significant tier 1 suppliers	232	88.56
High-risk suppliers	12	-
Non-tier 1 Suppliers	90	-
Significant non-tier 1 suppliers	51	-

To gradually reduce overall supply chain risks, we expanded our management scope to include non-tier 1 suppliers, identifying 90 such suppliers. Among them, 51 were further defined as significant non-tier 1 suppliers² and incorporated into our risk control measures to ensure stable supply chain operations.

5.3.2 Supply Chain Sustainability Management

Wistron has established a comprehensive sustainable supply chain management process that consists of five core steps: adherence to sustainability norms, sustainability risk assessments, sustainability assessment, corrective actions and capability building, and the implementation of reward and exclusion mechanisms. This mechanism is designed to ensure that every supplier complies with Wistron’s Code of Conduct and sustainability requirements, while effectively mitigating potential ESG-related risks. Through regular and comprehensive risk assessments and audits, Wistron not only monitors suppliers’ implementation but also provides professional guidance to help suppliers develop and execute targeted improvement action plans. In addition, through long-term collaboration and capability-building initiatives, Wistron supports suppliers in continuously enhancing their performance across environmental, social, and governance (ESG) dimensions. These efforts not only improve the overall sustainability performance of suppliers, but also strengthen Wistron’s leadership and influence within the global supply chain, ensuring the steady advancement of the entire value chain toward sustainability.

Sustainability Management Process



Compliance with Sustainability Standards

Supplier Code of Conduct

In advancing corporate sustainability, Wistron recognizes the critical impact of supply chain management on both society and the environment. To this end, Wistron has established a Supplier Code of Conduct as a foundation for supplier action in sustainability practices. This Code is aligned with the Responsible Business Alliance (RBA) Code of Conduct and the United Nations Guiding Principles on Business and Human Rights, covering five core areas: labor rights, health and safety, environmental protection, ethics, and management systems. The Code also includes specific requirements related to biodiversity, the prevention of deforestation, and land conservation, aiming to holistically enhance the sustainability of the supply chain. Wistron also incorporates the level of supplier compliance with the Code as a key evaluation criterion in procurement decisions to ensure alignment between supply chain partners and the Company’s sustainability goals.

In 2025, 100% of Wistron’s Tier-1 suppliers signed the Supplier Code of Conduct, demonstrating their full recognition of and commitment to Wistron’s sustainability standards. In addition, depending on the supplier category, Wistron further required the signing of the letter of agreement, the declaration of controlled hazardous substances confirmation and compliance, and the declaration of non-use of conflict minerals, all of which also achieved a 100% signing rate. These measures have not only strengthened Wistron’s governance capabilities within the supply chain but also promoted a shared commitment among partners to uphold higher standards of social and environmental responsibility.

Signing of the Supplier Code of Conduct

Year		2025 Performance	2025 Objectives
Tier-1 suppliers	Number of suppliers required to sign	421	-
	Percentage of signed suppliers (%)	100%	100%
New Suppliers	Number of suppliers required to sign	43	-
	Percentage of signed suppliers (%)	100%	100%

Supplier Integrity Management

Wistron is committed to building a responsible supply chain of the highest standards. Through its [Supplier Code of Conduct](#), the Company establishes clear behavioral norms and standards for its partners. All suppliers are required to complete training courses on Wistron’s anti-corruption policies, with a 100% completion rate. In addition, Wistron reinforces its commitment to ethical business practices and integrity during the annual supplier conference. The Company also maintains dedicated whistleblowing and grievance channels exclusively for suppliers, which are managed primarily by the Global Supply Chain Management unit. In 2025, there were no supplier-reported cases, and no contracts were terminated due to misconduct or corruption.



Sustainability Risk Assessment

In order to assess sustainability risks within the supply chain, Wistron conducts a two-phase risk investigation on suppliers. Through varying requirements at different stages, we aim to evaluate suppliers’ESG performance and identify potential risks within the supply base. The first phase focuses on comprehensive risk screening, while the second phase further identifies high-risk suppliers. For high-risk suppliers identified through the assessment process, Wistron initiates an assessment procedure, combining professional guidance with support to help suppliers develop and implement improvement plans. This approach enables effective control at the source of risk and helps reduce overall sustainability risks within the supply chain.

Active Assessment | Target: All Suppliers

To identify potential risks within the supply chain, Wistron conducts preliminary assessments and screening of suppliers. The evaluation covers multiple dimensions, including environmental, social, and governance (ESG) performance, business relevance, country or region of operation, industry type, and commodity characteristics. Through this process, suppliers with potential risks are preliminarily identified and brought under management to reduce overall supply chain risk.

Factor	Content
Environmental	- Review major negative events or illegal records related to environmental issues, including but not limited to excessive hazardous substances, air pollution emissions, water pollution emissions, improper disposal of waste and toxic substances, etc. - Evaluate potential negative impact factors related to environmental issues, such as high carbon emissions, non-local procurement leading to increased energy consumption and resource waste, etc.
Social	- Review major negative events or illegal records related to social issues, such as violations of labor rights or occupational safety, forced labor, etc. - Evaluate potential negative impact factors related to social issues, such as the disclosure of negative reports involving the living wage or impact on local communities.
Governance	- Review major negative events or illegal records related to governance issues, including corporate fraud, bribery or false financial reports, etc. - Evaluate potential negative impact factors related to governance issues, such as insufficient operational soundness or anti-competitive behavior.
Business relevance	For critical business categories, we conduct a preliminary assessment based on procurement amount and consideration of the irreplaceability of products and the pioneering nature of industry technologies.
Country/Region	Based on the location of the supplier, we include regional and high-risk country controls and consider geopolitics , conflicts, and risk identification of high-risk countries.
Sector	Based on industry and business attributes, we evaluate the resource intensity and labor requirements of service processes or those involving specific concerns.
Commodity	Based on product attributes and raw material composition, we seek to have comprehensive understanding of any potentially hazardous substances or high-energy-consuming materials.

Risk Assessment | Assessment Scope: Tier 1 and Non-Tier 1 Suppliers

To comprehensively understand the sustainability risks of existing suppliers, Wistron distributes a Sustainability Risk Self-Assessment Questionnaire to both Tier 1 and non-Tier 1 suppliers, requiring them to provide supporting documentation to gain deeper insights into their sustainability risks and management practices. The questionnaire covers five key sustainability dimensions: sustainability and operational risk management, supply chain and continuity of operations, environmental protection, human rights and labor protection, and occupational safety and health. Through this mechanism, Wistron is able to identify and manage sustainability risks across the supply chain and mitigate potential risks.

Suppliers with a score of less than 80 are defined as high-risk suppliers. In 2025, a total of 12 high-risk suppliers were identified. According to the results, the main sustainability risk factors in 2025 were concentrated in the areas of environmental protection and sustainability and operation risk management. In order to effectively mitigate the impact of these risk factors, Wistron will prioritize greenhouse gas inventory and certifications (ISO 50001 and ISO 14064-1) for critical and high-energy-consuming material suppliers. Other identified risk factors will be listed as items requiring guidance for remediation through assessment and improvement programs.

Dimension	Risk factors	Countermeasures
Environmental protection	Energy conservation and carbon reduction mechanisms for energy management have not been implemented (ISO 50001)	Engaged high-energy-consuming material suppliers to obtain ISO 50001 certification
	Uncertified greenhouse gas inventory certification management (ISO14064-1)	Engaged high-energy-consuming material suppliers to obtain ISO 14064-1 certification
	No statistics on Scope 3 greenhouse gas emissions generated by products or services	Engaged high-energy-consuming material suppliers in Scope 3 greenhouse gas inventory
	No statistics on Scope 1 greenhouse gas emissions generated by products or services	Engaged high-energy-consuming material suppliers in Scope 1 greenhouse gas inventory
Sustainability and operational risk management	Response plan management for business continuity has not been implemented	List as items requiring guidance for remediation

Sustainability Assessment

To comprehensively assess the implementation of sustainability practices among suppliers, Wistron adopts a diversified assessment approach, including both desk assessments and on-site assessments. On-site assessments are further categorized into 2nd party assessments, 3rd party assessments, and assessments conducted in accordance with industry standards. Wistron has also established annual targets and a long-term goal for 2030, providing clear direction for promoting sustainability in the supply chain over both the short and long term, thereby enabling continuous progress toward these objectives.

Category	Assessment Format	Approach	Scope	No. of Assessments in 2025	2025 Targets	2030 Targets
Desk	Desk assessments	Distribute self-assessment questionnaire on sustainability risks and request supporting materials	511 tier 1 and non-tier 1 suppliers	511	Conduct desk assessments for all significant suppliers	Conduct desk assessments for all suppliers (incl. tier 1 & non-tier 1)
On-site assessments	2nd party assessments	On-site assessments and review operations are performed by Wistron for significant tier 1 suppliers, and by tier 1 suppliers or consultants for non-tier 1 suppliers	283 significant tier 1 suppliers and significant non-tier 1 suppliers	168	Conduct on site assessment for all significant suppliers	Conduct on site assessment for all significant suppliers
	3rd party assessments	Third-party verification		3		
	Industry Standard	Assessments based on RBA standards		112		
	Total number of on-site assessments			283	100%	100%

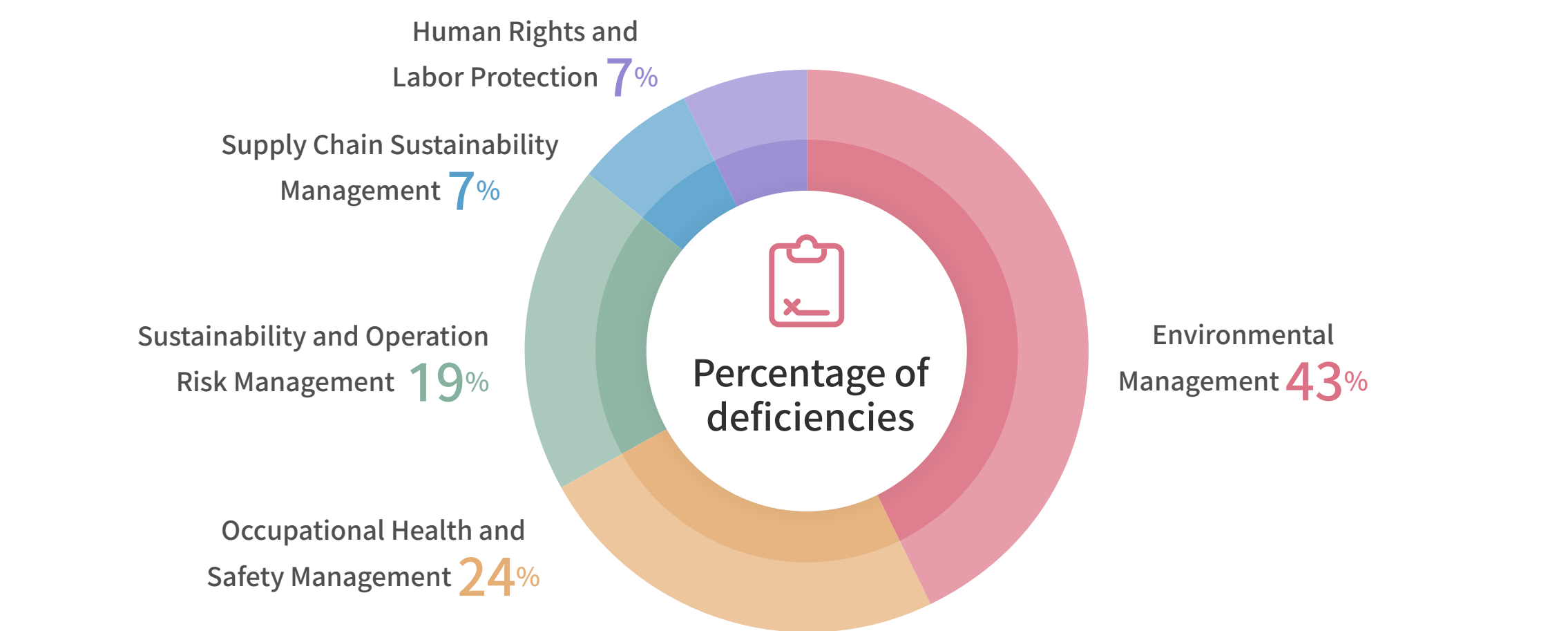


Corrective Action/Improvement Plans

To enhance the sustainability performance of suppliers, Wistron provides counseling measures for deficiencies identified in assessments, including on-site and remote support to assist suppliers in developing and implementing improvement plans. If the supplier is unable to complete the improvements within two months, they may submit another assessment application for a second assessment to confirm the implementation of the improvement plan. However, if a supplier fails to pass the second assessment, they must wait six months before reapplying. During this period, Wistron will evaluate the feasibility of using alternative materials or consider replacing the supplier. If immediate substitution is not feasible due to urgent supply requirements, the replacement will proceed once an alternative is in place. For suppliers unable to meet improvement requirements within two years, Wistron will gradually reduce procurement volume until the partnership is terminated or the supplier is disqualified. In 2025, all assessed suppliers completed the required improvements within the specified timeframe, and no partnerships were terminated due to non-compliance.



Note: Includes 12 High-risk suppliers



Supplier Assessment Corrective/Improvement Actions

Dimension	Topic	Corrective/Improvement actions
Sustainability and operation risk management	Business Continuity Management/ Sustainability Disclosure	- Develop an annual schedule for BCP exercises, ensuring critical personnel are trained, and record outcomes with subsequent improvement measures. - Systematically consolidate and document existing business continuity and risk management materials. - Establish verifiable operational continuity capabilities to enhance client trust, meet specific customer or contract requirements, and reduce the risk of major operational disruptions.
Supply chain sustainability management	Supplier selection	- Establish standardized supplier scoring criteria and selection procedures, complemented by training to ensure procurement processes align with sustainability requirements and standards. - Integrate sustainability factors such as energy, carbon, and water management into supplier selection criteria to progressively enhance maturity of ESG management across the supply chain. - Ensure all procurement, quality assurance, and supply chain personnel clearly understand and correctly implement ESG requirements to improve sustainability performance of the overall supply chain.
Environmental management	Energy management/ Greenhouse gas management	- Develop and implement carbon emission control procedures, clearly defining departmental responsibilities, reduction methods, and implementation steps, with monitoring, recording, and audit mechanisms to ensure enforceability and continuous improvement. - Publish annual energy-saving and emission-reduction targets and implementation plans, specifying indicators, responsibilities, timelines, and resources, with tracking and reporting mechanisms for performance evaluation and improvement.
Human rights and labor protection	Communication channel/Non-discrimination	- Increase post-training assessments and random checks, establishing a regular retraining system to ensure employees understand anti-discrimination policies and communication channels. - Enhance employee satisfaction surveys and feedback channels, while strengthening privacy protection for employees and external complainants.
Occupational safety and health	Occupational safety and health/ Compliance management	- Establish and improve safety operating procedures, implement hazard identification and risk control measures to reduce accidents and occupational illnesses, ensuring workplace safety and employee health. - Set standards for equipment placement and signage, inspect fire safety equipment and locations, and audit on-site equipment periodically.

Driving Supplier Excellence with Sustainability Performance

To encourage suppliers to implement sustainable practices and enhance their sustainability performance, Wistron conducts sustainability performance evaluations of suppliers and implements a preference and exclusion mechanism in accordance with relevant management procedures.

Preference mechanism	Exclusion mechanism
Suppliers with outstanding sustainability performance ratings receive higher order allocations, and are granted opportunities to participate in new projects. They are also recognized and honored as Outstanding Suppliers during the annual Partner Conference.	Suppliers with poor sustainability performance will have their eligibility for new project participation suspended and procurement volumes reduced. Suppliers that fail to make necessary improvements within two years will be removed from the procurement list and disqualified as Wistron suppliers.
2025: 10 suppliers received an Outstanding Supplier Award and 8 suppliers received more Wistron orders for outstanding sustainability performance	2025: 1 supplier was placed on the exclusion list due to poor sustainability performance after recurring non-conformities were identified following an RBA audit and implementation of a CAP

Supplier Sustainability Evaluation

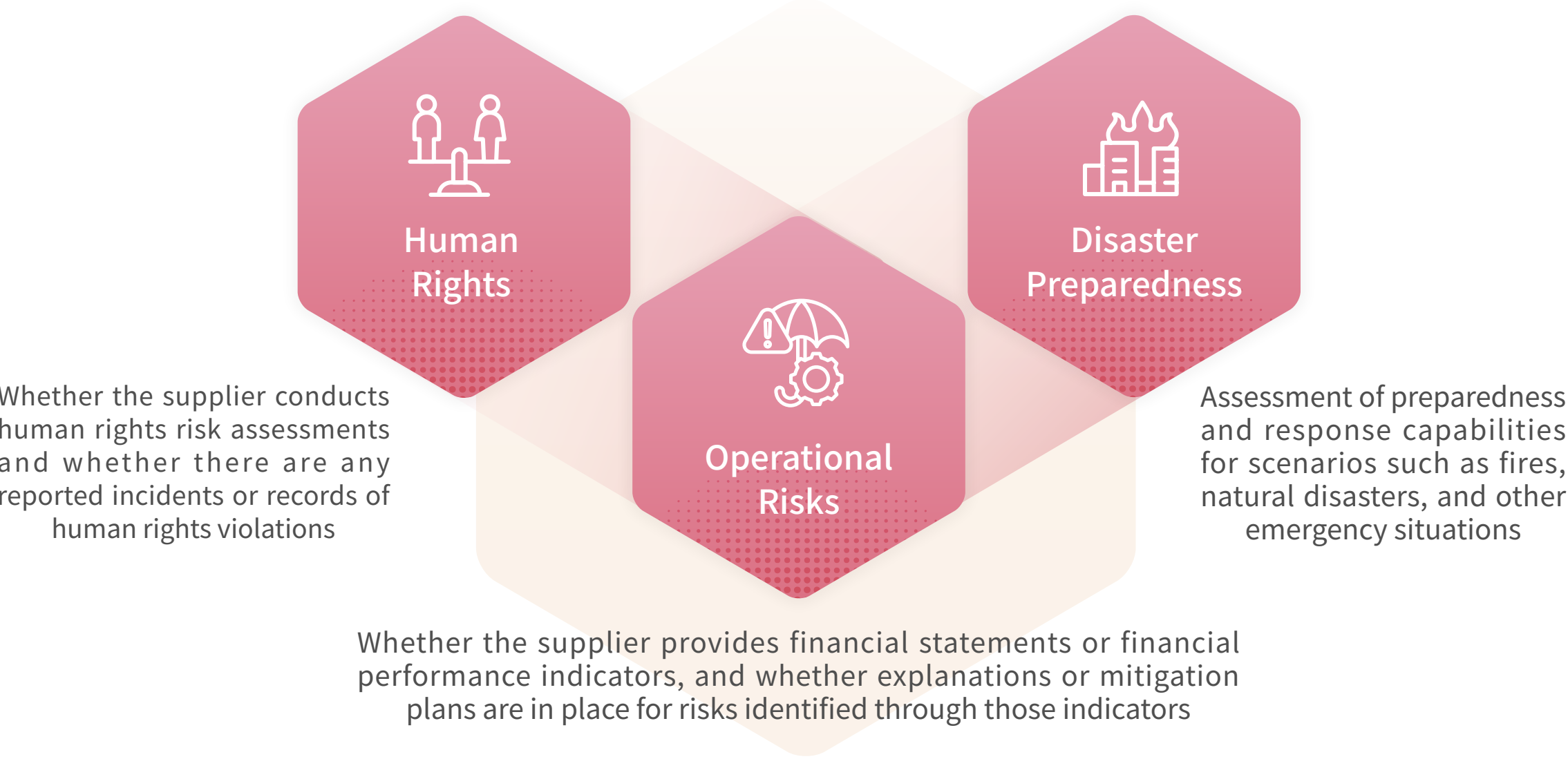
Wistron has set ESG evaluation thresholds for new and existing suppliers. Those applying to be Wistron suppliers are required to sign a Code of Conduct and pass the following four certifications:



Scope	Assessment Tool	ESG Weighting	ESG Assessment Criteria
New suppliers	Supplier quality system evaluation form	13.33%	Responsible Business Alliance (RBA) Code of Conduct, labor standards, health and safety, environmental standards, business ethics, and management systems
Existing suppliers	Supplier performance evaluation including quality, technology, cooperation, delivery capability, price, and ESG performance	20%	Quarterly review of ESG sustainability activity, ISO 14064-1 certification annual review, ISO 50001 certification annual review, annual ESG audit score, and major missing events of ESG sustainability on-site assessment

ESG Risk Management and Mitigation Plans

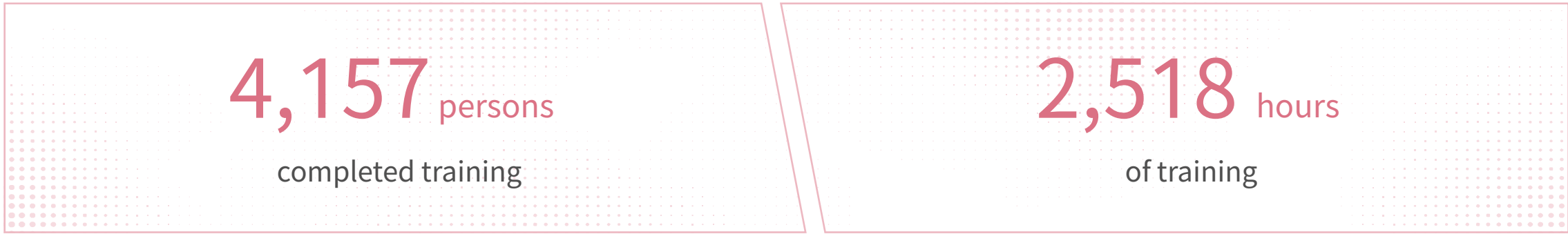
In addition to the existing supplier performance evaluation framework, Wistron incorporates ESG risk management and mitigation plans into supplier assessments, covering three key risk areas:



Capacity Building

Buyer Education Training

To ensure procurement staff (including personnel from buyers, logistics, quality assurance, and other supply chain-related departments) fully understand supplier management and sustainability processes, as well as their roles, Wistron implements systematic training to enhance employees’ expertise in ESG topics. The training covers fundamental human rights issues such as the prohibition of forced labor (including servitude, debt bondage, and human trafficking) and gradually strengthens professional capabilities needed for sustainability management for Wistron’s business scope. Through this training, employees are equipped to drive sustainable supply chain strategies and ensure effective implementation in daily operations and interactions with suppliers. In 2025, Wistron continued to collaborate with the ESG Sphere Course Review Committee to develop a series of ESG-related training modules. A total of 4,157 employees completed the training, amounting to 2,518 hours of learning.



Supplier Education Training

To support suppliers in adopting ESG-aligned strategies and actions in their operations—and to strengthen the overall resilience and sustainability of the supply chain—Wistron continues to offer relevant training through its online supplier education platform. These courses aim to enhance suppliers’ awareness of sustainable development principles and reinforce partnerships with suppliers. In 2025, in addition to the annual mandatory course on the Supplier Code of Conduct, Wistron added two new mandatory courses—RBA Standards on Prohibition of Forced Labor and ISO 37001 Anti-Bribery Management Systems. The former supports suppliers in understanding the importance of RBA human rights issues, while the latter ensures suppliers recognize the key role of ethical management in earning customer trust and advancing sustainability competitiveness. A total of 421 tier 1 suppliers completed online training, representing a 100% training completion rate.

Existing	New
Annual Course on Supplier Code of Conduct Covers Wistron’s core requirements	ISO 37001 Anti-Bribery Management Systems Covers the importance of ethical management in advancing sustainability competitiveness RBA Standards on Prohibition of Forced Labor Helps suppliers recognize the importance of RBA human rights issues

Partner Conference/Sustainability Sharing Forum/Lectures

In 2025, Wistron focused on the theme of “Make an Impact,” hosting its annual Partner Conference, ESG sharing sessions, sustainability lectures, and various events to strengthen supplier awareness over sustainability and resilience, enhance ESG capabilities, and deepen sustainability partnerships across the supply chain.

Events	Scale	Description
Sustainability Sharing Forums	302 supplier participants	Focused on carbon reduction targets and performance tracking, EPEAT and PFAS management strategies, ISO 37001 anti-bribery, ISO 20400 sustainable procurement, zero-waste-to-landfill initiatives. Case sharing included measurement and verification case studies of energy savings and carbon reduction from lighting and HVAC system upgrades from three benchmark suppliers. Promoted Wistron’s sustainability management, anti-corruption policies, greenhouse gas inventory, and water risk management. Also highlighted industry cases of significant losses from bribery and corruption to raise awareness among suppliers.
Supplier Sustainability Evaluation Lecture	94 participants from 48 suppliers	Held on August 26 and September 2 at Zhongshan and Chongqing sites, respectively. Covered ESG policies, sustainable procurement requirements, and performance evaluation criteria. Conducted training on prohibition of forced labor. Included interactive ESG board game Wi-Thrive to enhance engagement and deepen understanding of sustainability topics.



Establishing A Segmented Supplier Carbon Management Promotion Strategy

Starting from 2021, annual greenhouse gas inventory results from suppliers are collected. Upon analysis, it was found that suppliers exhibit varying degrees of capability in carbon inventory and reduction. Consequently, a classification management system has been implemented, categorizing suppliers based on their level of significance (determined by factors such as revenue and material substitutability) and carbon inventory capabilities. Tailored project plans are provided to suppliers in different categories, along with necessary assistance resources, experience-sharing courses, and consulting resources, to ensure their progressive advancement towards carbon neutrality. In 2025, suppliers were encouraged to adopt renewable energy, particularly solar power, optimize manufacturing processes, and improve energy efficiency through facility and equipment upgrades, thereby reducing carbon emissions.

Category		Carbon management strategies for suppliers		
I		• Conduct greenhouse gas inventory and factory-side self-inventory		
II		• Third-party verification for scope 1 and scope 2 GHG inventory • Scope 3 GHG inventory • ISO 50001 energy management system certification for high-energy-consuming material suppliers • Establish a carbon reduction project with an annual reduction of 4.2%		
III		• Third-party verification for scope 1+2+3 GHG inventory • ISO 50001 energy management system certification for high-energy-consuming material suppliers • Join the SBTi commitment or set up a 4.2% annual carbon reduction project		
Level of supplier significance	High	II	II	III
	Medium	I	II	III
	Low	I	I	II
		Low	Medium	High
Supplier's Carbon Inventory Capabilities				

Building Supplier Carbon Management Capabilities

Wistron conducted a comprehensive inventory of Scope 3 greenhouse gas emissions, with results indicating that upstream raw material procurement accounts for the highest share of emissions. In response, Wistron launched a carbon management capacity-building program tailored to different categories of suppliers. The program covers carbon inventory training, verification mechanism enhancement, the introduction of Science Based Targets (SBTi) initiative emission reduction targets, and collaborative carbon reduction projects. In 2025, Wistron initiated four carbon management projects and engaged in in-depth collaborations—lasting over six months—with 352 suppliers (including 227 significant suppliers), continuously enhancing the carbon management capabilities of supply chain partners and jointly advancing emission reduction targets.

Category	Project	Cooperative partner-Significant Suppliers	Details	Benefits & Impacts
I	Carbon inventory capacity building plan	Tier-1 suppliers	- Support suppliers in building carbon accounting capabilities - Collect supplier carbon inventories to complete supply chain emission data	- Completed carbon inventory data and sustainability survey for 352 suppliers - Coverage (by procurement amount): 90.11%
II	High energy consuming material suppliers' verification program	High energy consuming material suppliers	Since 2022, we have been consistently expanding our categories, selecting critical high energy-consuming material suppliers to promote ISO 14064-1 and ISO 50001 certification	Out of the 52 suppliers selected for promotion, 50 attained ISO 14064-1 certification, while 43 achieved ISO 50001 certification
		High energy consuming material suppliers	Wistron joined government-led low-carbon transition initiatives by leveraging the “big leads small” approach, collaborating with 30 suppliers in total. Among them, Wistron worked closely with 7 suppliers to establish carbon reduction mechanisms and promote low-carbon practices. These efforts included sharing energy-saving technology improvement strategies, commissioning research institutes to conduct supplier energy audits and diagnostics, and establishing project verification mechanisms for energy conservation and carbon reduction. Technical support was also provided to promote industrial energy efficiency improvements and carbon management tools	- We collaborated with seven suppliers to jointly propose energy-saving improvement projects, resulting in a cumulative reduction of 14,344 tCO₂e. - Completed carbon inventory and sustainability data surveys for 23 suppliers, serving as a foundation for subsequent evaluation and project analysis - Completed the Energy Conservation & Decarbonization Handbook to promote decarbonization among suppliers and extend our influence
			Encourage suppliers to conduct energy conservation and decarbonization projects	14 suppliers launched energy conservation and decarbonization projects - Total projects: 60/ Total carbon reduction: 43,476 tCO₂e
III	SBTi initiative commits to promote	Suppliers with high carbon inventory maturity	Collaborate with customers to target and encourage suppliers in high energy consuming industries to participate in SBTi and respond to CDP questionnaires	41 suppliers have joined SBTi & 120 suppliers have completed CDP questionnaires

Supplier Circular Economy Capacity Building Project

Amidst the global push for a circular economy, Wistron remains committed to safeguarding natural life and forests by fostering communication and collaboration with suppliers. This focus enables the fulfillment of biodiversity and non-deforestation pledges, while also encouraging suppliers to obtain Zero Waste to Landfill certification, and simultaneously reducing the Earth’s environmental burden. Furthermore, it enhances suppliers’ sustainability awareness and capabilities to adapt to evolving sustainability trends.

Supplier Partnership Projects	Details	Qualitative Benefits	Quantitative Benefits
Integrated Resource Utilization (waste diversion/recycling/ scrap repurposing)	- Eliminates cost of waste disposal - Lower waste transportation & disposal fees: Waste to incinerators/landfills significantly reduces from waste diversion (recycling/reuse), directly reducing costs of waste transportation and disposal - Lower waste disposal fees: Recycling generally costs less than waste disposal - Revenue from resource recovery and sales of renewable resources: Generate non-operating income by diverting and selling recyclable materials with residual value (paper, metals, and selected plastics) which were previously disposed (without sorting) - Scrap repurposing program: Convert irregular scrap materials into value-added products by cutting and assembling them into standard paperboard; processing them into cushioning pads, dividers, and small-sized cartons; and shredding unusable scraps for use as recycled paper feedstock	Environmental Benefits - Reduced landfill disposal: Diverts waste from landfills, reducing land use requirements and pollution risks - Lower carbon emissions: Improves resource recovery and conversion efficiency, contributing to the reduction of Scope 3 greenhouse gas emissions - Advances the circular economy: Extends material life cycles through reuse and recycling, reducing demand for virgin raw materials Economic Benefits - Lower waste management costs: Optimizes waste handling processes and reduces treatment and disposal expenses - Enhanced brand value: Achievement of UL 2799 certification enables suppliers to demonstrate environmental performance publicly and strengthen ESG performance	- Waste recycled and reused: 4,465t - GHG emissions avoided through Zero Waste to Landfill initiatives: 3,925 tCO₂e - Direct economic benefits from suppliers: NT\$18.5M - Number of key suppliers obtaining UL 2799 certification: 20 suppliers
Manufacturing Circularity (wood pallets, regrind materials, and turntables)	Closed-loop pallet system (including repairing damaged pallets for reuse and reducing landfill disposal costs), reprocess and reuse plastic regrind materials, and closed-loop PE turntables		
Process Waste Reuse for Tool Production	Use metal/plastic scraps to replace raw materials for tool production	Management Benefits - Standardized management processes: UL 2799 provides clear classification and calculation standards, supporting the establishment of consistent waste management systems - Greater transparency and stakeholder trust: Third-party audits and certification help demonstrate sustainability commitments to investors, customers, and the broader public	

KPIs for Supplier Sustainability

- Supplier audits and support: 283 significant suppliers were audited and 100% of them implemented corrective actions within the designated time for any deficiencies found;
- Supplier training: 100% of the 232 significant tier 1 suppliers completed mandatory online courses (Supplier Code of Conduct, RBA Standards on Prohibition of Forced Labor, and ISO 37001 Anti-Bribery Management);
- Supplier capacity building in carbon management and circular economy projects: Promoted carbon management to 227 significant suppliers and circular economy to 20 suppliers through six months of in-depth collaboration, with a capacity building success rate of 81.98%;

Wistron provided support to significant suppliers for the implementation of corrective action against deficiencies found in audits as well as education and training for capacity building with carbon management and circular economy projects, with a 100% coverage rate.

KPI		2025 Performance	2025 Targets
Corrective Action/Improvement Plans		100% (No. of significant suppliers: 283)	100%
Supplier Education Training		100% (No. of significant tier 1 suppliers: 232)	100%
Capacity Building	Carbon Management	227 significant suppliers	81.98%
	Circular Economy	20 significant suppliers	

Green Supply Chain Management

A green, transparent, and circular supply chain encompasses all the essential elements of a modern sustainable supply chain. Wistron’s green supply chain management covers the following:

- Green Design: Incorporates RoHS standards (Restriction of Hazardous Substances) at the design stage to ensure environmental compliance. Wistron products comply 100% with RoHS and REACH regulations across all countries and 100% of suppliers have signed supplier hazardous substance declarations.
- Green Procurement: In accordance with green design requirements, priority is given to procuring green materials, including products and suppliers with green label and energy-efficiency certifications, to reduce environmental impacts.
- Green Manufacturing: Partners with low-carbon suppliers to implement carbon reduction strategies and promote sustainable production. In 2025, 21 suppliers participated in carbon reduction projects, with 20 suppliers achieving Zero Waste to Landfill certification.
- Green Packaging: Reduces and reuses packaging materials while ensuring reliability. Prioritize suppliers with Forest Management (FM) and Chain of Custody (CoC) certifications for shipping materials to ensure sustainable sourcing. 100% of Wistron’s key packaging suppliers are FSC-certified.
- Green Transportation: Utilizes low-emission, energy-efficient, and smart logistics solutions to support carbon reduction. In 2025, the Vietnam site reduced truck trips by 6,164, reducing trips by 1.29 million kilometers and approximately 76% of emissions.
- Green Recycling: Promotes the use of sustainable materials. Low-carbon notebooks contain 40.2% PCR material, and 96% of packaging materials are recyclable or reusable; while server products utilize 90% recycled steel (SGCC).

These measures ensure that every stage of the green supply chain helps mitigate environmental impacts and supports the company’s progress toward sustainable development goals.

5.3.3 Conflict Minerals Management

To achieve responsible and sustainable procurement practices, Wistron has established a conflict minerals policy and a responsible mineral sourcing management process. Wistron is committed to conducting due diligence on suppliers in accordance with the Organization for Economic Co-operation and Development (OECD) Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas or an equivalent internationally recognized due diligence framework. Wistron is committed to cooperating exclusively with smelters and refiners that comply with global standards and strictly prohibits the procurement of tantalum, tin, tungsten, gold (3TG), and cobalt from conflict-affected or high-risk areas, thereby preventing any direct or indirect contribution to human rights violations or armed conflicts in these regions.

Key Practices:

1. Establish and implement a responsible minerals sourcing management process in accordance with the guidance and tools developed by the Responsible Minerals Initiative (RMI); and encourage suppliers to establish internal policies, implement mineral source traceability mechanisms, and monitor their supply chain.
2. Utilize RMI reporting templates (CMRT/EMRT) and Wistron's internal SQP (supplier questionnaire platform) to systematically conduct due diligence, data collection, and audits. Suppliers are required to disclose the sources of minerals used in their products and sign the Conflict Minerals Statement. In 2025, all 407 Tier-1 suppliers completed the declaration process, achieving a 100% declaration rate¹.
3. Conduct annual reviews of smelter and refiner lists based on the latest RMI conformant smelters list to ensure continued compliance with international standards, regulatory requirements, and customer expectations.
4. Apply the Reasonable Country of Origin Inquiry (RCOI) process and reference the RMI's list of conformant smelters or refiners (SORs) to trace mineral origins, identify countries of origin, and support risk assessment activities.
5. Management of conflict mineral use uncovered from supply chain: If not mandatory, Wistron will require suppliers to halt procurement of the conflict mineral in question and switch to RBA-compliant sources (non-conflict or recycled) and provide related evidence. If mandatory, Wistron will ask suppliers to propose a phase-out plan or improvement plans to gradually reduce risks.
6. Wistron has begun incorporating recycled minerals with equivalent material properties, including recycled copper, into certain products to gradually reduce reliance on virgin minerals that may pose conflict mineral risks.

Note: Since 2023, Wistron has labeled its product packaging with "CMRT-Free" to clearly demonstrate its commitment to not using conflict minerals; signing rate of the "Declaration of Conflict Mineral-Free" excludes logistics providers.



5.4 Operating Capability

5.4.1 Operational Achievements and Future Outlook

Wistron drives industry transformation through technological innovation. In the face of intense global market competition, we optimize production processes, enhance manufacturing efficiency and product quality, and reduce environmental footprint through automation, digital transformation, and Digital Twin technologies. To address climate change and carbon reduction challenges, we actively adjust business models, expand investment in advanced technologies and the circular economy, and promote resource circulation and full lifecycle management. To mitigate the impact of geopolitical risks, Wistron continuously expands production sites and dynamically allocates capacity based on customer demand. We also assess internal and external environmental changes to strengthen supply chain resilience. By embedding sustainability into our corporate strategy, we transform environmental and social challenges into opportunities for innovation and growth, aiming to generate long-term, cross-generational sustainable impact.

Wistron’s consolidated revenue in 2025 was NT\$2.2 trillion. The net operating profit was NT\$78.6B. The net profit after tax was NT\$27.4B. The revenue and profit increased from 2024 and the net profit after tax reached a 10-year high.

Financial Performance Indicators for the Past 4 Years

Unit: NT\$1M

Year/Item	2022	2023	2024	2025
Net revenues	984,619	867,057	1,049,256	2,186,523
Operating income	27,472	27,390	38,980	78,553
Net profit after tax	11,162	11,472	17,446	27,408

Note: Refer to [Appendix 6.2](#) for the complete financial performance list.

5.4.2 Tax Policy

The Wistron Board of Directors serves as the highest decision-making and supervisory body for the Company’s tax affairs. It is responsible for approving tax strategies and regularly reviewing their implementation to ensure that tax policies are closely aligned with the Company’s business objectives and sustainability strategies. The Board-approved [Tax Policy and Management Guidelines](#) serve as the foundation for the Company’s tax governance. The Company adopts a reasonable tax management structure to ensure an appropriate tax burden in all key operating countries. This approach aims to support social and economic stability and promote the sustainable development of the Company’s operations.

Tax Information in the Past Two Years

Unit: NT\$1,000

Item	2024	2025	Average
Net profit before tax	39,975,476	76,257,264	58,116,370
Income tax expenses	9,339,245	18,484,761	13,912,003
Effective income tax rate (%)	23.36	24.24	23.94
Income tax paid	5,559,333	13,807,719	9,683,526
Cash tax rate (%)	13.91	18.11	16.66

Note: Please refer to Wistron’s [2025 Consolidated Financial Report](#) for related information.

Income Tax Paid (received) in Various Regions Between 2024 and 2025

Unit: NT\$1,000

Year	2024		2025	
Region	Amount	Percentage (%)	Amount	Percentage (%)
Asia	4,938,960	89	11,392,312	83
Americas	741,271	13	2,277,280	16
Europe	(120,898)	(2)	138,127	1
Total payment	5,559,333	100	13,807,719	100

5.4.3 Policy Influence

Wistron actively builds close collaborations with cross-industry and interdisciplinary groups and organizations, engaging deeply as a member to expand platforms for dialogue and broaden the scope of participation. Through collaboration with these organizations, Wistron stays informed of the latest international trends and developments, supporting the Company’s continued development. In 2025, Wistron participated in the following organizations and associations:

Category	Organization or Trade Association
Innovation	• Taiwan Electrical and Electronic Manufacturers’ Association • Taipei Computer Association • The Allied Association for Science Park Industries (ASIP) • Taiwan Industry-Academia Research for Collaboration-Integration-Development Association
Medical	• Taiwan Assistive Technology and Long-Term Care Industry Association
Others	• Regular member of the Responsible Business Alliance (RBA) • Member of the Gap of Learning & Field • Member of the CommonWealth Sustainability League • Member of the Business Council for Sustainable Development of the Republic of China (BCSD Taiwan) • Epoch Foundation



