3 Corporate Stable Operations

3.1 Corporate Governance 23

3.2 Ethical Corporate Management and Legal Compliance 27

3.3 Risk Management 29

3.4 Information Security and Privacy Protection 32

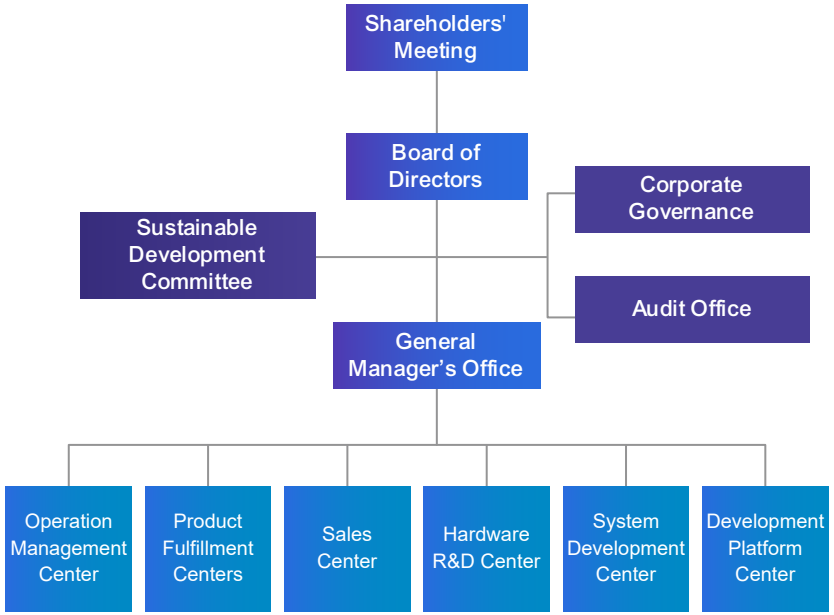
3.1 Corporate Governance

Item	Content
Policies, Commitments, and Importance	Giga Computing understands that good corporate governance is a crucial foundation for sustainable business operations. We adhere to capital market regulations and will continue to strengthen the functions of the Board of Directors while continuously optimizing the Company's governance mechanisms. At the same time, to ensure effective communication and coordination among relevant parties, the Company has established good communication channels and mechanisms with the internal audit managers. The Chairman of the Board reports on the communication status with the internal audit managers to the shareholders' meeting.
Responsible Unit	General Manager's Office, Financial & Accounting Division
Action Plan	1. To ensure effective communication and supervision, board meetings are held at least once every quarter, including the communication among the internal audit managers. The internal audit situation shall be explained in detail in the report of the Board of Directors, and the audit plan for the following year shall be approved at the end of the year. 2. Directors regularly participate in continuing education courses and will continue to undertake appropriate courses in the future based on market and governance needs. 3. In the future, the Board of Directors will be responsible for establishing performance evaluation criteria for directors and managers and for regularly assessing the achievement of their performance targets as a basis for determining individual remuneration. 4. In the future, the Company plans to report the ESG-related performance of senior managers to the Board of Directors or governance units and gradually link senior managers' remuneration to corporate ESG performance evaluation results to strengthen sustainability governance and accountability.
2025 Performance	1. Establish an independent audit unit to supervise the Company's various operating activities through the internal audit mechanism. 2. Board of Directors' meetings were held during the year, with an average attendance rate of 86.67%. 3. The average number of training hours per director is 6 hours.
Grievance Mechanism	Stakeholders can directly communicate with the Company through the official website. Material company events are also occasionally announced on the official website and published on the MOPS as required by the Company Act.

3.1.1 Corporate Governance Structure

The Board of Directors is the highest governing body of the Company, which consists of one Chairman, who serves as the head of the Board internally and represents the Company externally. In addition to executing business operations in accordance with laws, regulations, the Articles of Incorporation, and resolutions of the shareholders' meeting, the Board of Directors is vested with authority including, but not limited to, the following: the Company's annual and semi-annual financial reports; evaluation of the effectiveness of the internal control system; appointment or dismissal of CPAs; appointment and dismissal of managers; and strategic plans. All of the foregoing matters must be approved by the Board of Directors to ensure that the Company's long-term development aligns with its vision and values. In 2025, the average attendance rate of the Board of Directors' meeting was 86.67%.

The General Manager, entrusted with responsibilities by the Board of Directors, serves as the highest leader of the management team, overseeing the overall business and operational direction of the Company. All centers and units under its supervision are required to report their operational status to the General Manager on a monthly basis. To enhance the corporate governance structure, Giga Computing has established the Sustainable Development Committee, the Corporate Governance Unit, and the Audit Office. The Sustainable Development Committee oversees the implementation of the Company's sustainability initiatives, the Corporate Governance Unit ensures the effective operation of the Company, and the Audit Office is responsible for evaluating and monitoring internal controls and procedures. Among them, the Corporate Governance Unit and the Sustainable Development Committee did not commence operations in 2025. Moving forward, we will gradually initiate the functions of these governance units according to the Company's plan, aiming to strengthen the governance mechanisms.



3.1.2 Board Diversity and Continuing Education

The Company follows the board member diversity policy and, based on the Company's operational characteristics and needs, formulates appropriate background diversity guidelines to ensure the implementation of corporate governance, enhance the board's functions, and improve its structure. Through diverse recruitment, we have attracted talent with varied professional backgrounds, skills, and industry experience, continually enhancing corporate governance and operational synergies.

The Company currently has five directors, aged between 61 to 70, with expertise in business, technology, and industry marketing. Each director brings extensive experience in their respective industries. In the future, to promote the sound development of the Board of Directors' composition and structure, Giga Computing will continue to implement the board diversity policy to enhance corporate governance effectiveness and management performance.

The Company encourages board members to pursue continuing education to enhance their professional skills and knowledge, stay updated on current industry and regulatory changes, and apply the latest management strategies. This approach aims to broaden their perspective on corporate governance and improve their ability to assess and respond to the broader market environment. This year, board members participated in training courses, with an average of 6 hours of continuing education.

■ **2025 Continuing Education of Directors**

Course Offering Unit	Course Title	Course Hours (hours)	Number of Trainees	Training Hours (hours)
Accounting Research and Development Foundation	Strategies for High-Net-Worth Individuals in the Era of Global Tax Enforcement	3	5	15
	Corporate Governance and Securities Regulations: Interpretation of Financial Statements and Fraud Case Analysis	3	5	15
Total Training Hours				30 hours

Board Members and Their Backgrounds

Job Title	Name of Director	Gender	Age	Period of Election	Term of Office	Main Education Experience	Other Important Positions
Chairman	Yeh, Pei-Chen	Male	61-70	2025.05.16	3 years	EMBA, National Chengchi University Minghsin University of Science and Technology	Chairman of GIGABYTE Technology President of GIGABYTE Technology Chairman of Giga Investment Corp. Director Representative of G-Style Chairman of Giga-Trend International Investment Group Ltd. Director of Walsin Technology Corporation Director Representative of BYTE International Co., Ltd. Director of Albatron Technology Co., Ltd. Director Representative of Shun On Electronic Co., Ltd. Director Representative of Spirox Corporation Director Representative of AMIDA Technology, Inc.
Vice Chairman	Lee, E-Tay	Male	61-70	2025.05.16	3 years	Master of Computer Engineering of California State University (CSU), Chico	Director of GIGABYTE Technology Group General Manger of GIGABYTE Chairman of GIGAIPC Co., Ltd. Director Representative of Giga-Trend International Investment Group Ltd. Director Representative of BYTE International Co., Ltd. Director Representative of MyelinTek Inc. Independent Director of PCL Technologies, Inc.
Director	Yang Hsueh-Ching	Female	61-70	2025.05.16	3 years	National Taipei University of Business	Director Representative of GIGABYTE Technology Director Representative of Giga Investment Corp. Supervisor Representative of BYTE International Co., Ltd. Director Representative of CLOUDMATRIX Ltd.
Director	Ma, Mou-Ming	Male	61-70	2025.05.16	3 years	Electronic and Computer Engineering, National Taiwan University of Science and Technology	Director Representative of GIGABYTE Technology Senior Vice President of GIGABYTE Technology Director Representative of Giga Investment Corp. Director Representative of Giga-Trend International Investment Group Ltd. President of MyelinTek Inc.
Director	Tseng, Chun-Ming	Male	61-70	2025.05.16	3 years	Minghsin University of Science and Technology	Director Representative of GIGABYTE Technology Senior Vice President of GIGABYTE Technology Chairman of Selita Precision Co., Ltd.

3.1.3 Nomination and Selection of Board Members

According to Giga Computing's "Articles of Incorporation," the Company shall have five to seven directors, with a term of three years. Directors are elected by the shareholders' meeting from among individuals with legal capacity and may be re-elected consecutively. If the term of a director expires without re-election being held, the director's duties will be extended until the newly elected director assumes office.

In addition, according to "Articles of Incorporation," the Board of Directors is composed of the directors and requires the attendance of more than two-thirds of them. A Chairman and a Vice Chairman are elected by a majority vote among the attending directors. The Chairman represents the Company externally and oversees the Company's operations internally, while the Vice Chairman assists in these duties. Currently, the Chairman of the Company is Mr. Yeh, Pei-Chen, the Vice Chairman is Mr. Lee, E-Tay, and the General Manager is Mr. Hou, Chih-Jen.

In order to avoid conflicts of interest, any director who has a stake in the matter being discussed, whether it involves themselves or the legal entity they represent, must disclose the key details of their interest during the board meetings. Directors with a conflict of interest must recuse themselves from both discussion and voting on the matter and shall not act as proxy for another director in exercising voting rights.

3.1.4 Functional Committees

Functional committees play an important role in corporate governance, particularly in ensuring the effective operation of the Company, enhancing transparency, and reducing risks. In 2025, the functional committees at Giga Computing have not yet commenced operations. Moving forward, the Company plans to gradually establish relevant management policies and procedures based on its plans to strengthen internal controls, improve transparency, and better align with corporate governance best practices. Through such a process, the Company can establish a more comprehensive governance structure, thereby strengthening the foundation for its long-term business success.

3.1.5 Performance Evaluation

Since Giga Computing is currently a non-public company, no performance evaluation of the Board of Directors was conducted in 2025. In the future, as the internal governance structure becomes more complete, we plan to introduce performance evaluations for the Board of Directors to help the Company assess the performance and effectiveness of board members, identify potential areas for improvement, and enhance the board's operational efficiency and decision-making quality, thereby promoting the Company's competitiveness and sustainable development capabilities.

3.1.6 Remuneration Policy

Giga Computing determines the performance evaluations and remuneration decisions for its directors and managers by referencing industry standards and practices. At the same time, we consider the responsibilities held by individuals, their achievement of personal goals, performance in other positions, and the remuneration provided for similar roles in recent years when conducting a fair salary evaluation. Additionally, we assess the reasonable correlation between individual performance, company operational performance, and future risks, while also considering the achievement of the Company's short-term and long-term business goals and its financial status.

The Company determines the individual salary and remuneration amounts for directors and managers based on the annual and long-term performance goals set and achieved, in accordance with the salary and remuneration policies, systems, standards, and structure. Through this process, we ensure that the performance evaluations and remuneration decisions for directors and managers adhere to reasonable standards while protecting the Company's interests. This also demonstrates our commitment to regular reviews and transparency in our remuneration system.

In response to Giga Computing's emphasis on sustainable development, the Company plans to report ESG-related performance to the Board of Directors or governance units in 2026 and gradually link senior managers' remuneration to corporate ESG performance evaluation results to strengthen sustainability governance and accountability.

■ Remuneration Policy

Directors	Managers
The directors' remuneration at the Company is allocated according to the provision of the GIGABYTE Group's "Articles of Incorporation," Note 1 with the remuneration structure as follows: 1. Remuneration: Including directors' salary, duty allowances, severance pay, various bonuses, incentives, etc. 2. Pension 3. Remuneration to directors: The amount of remuneration to directors approved for distribution by the Board of Directors in the most recent year. 4. Business execution expenses: The recent annual board-related business execution expenses include transportation fees, special allowances, various subsidies, and the provision of company vehicles.	In accordance with Giga Computing's "Salary Management Procedures," "Employee Performance Evaluation Procedures," "Business Unit Financial Performance Calculation and Evaluation Principles," and "Performance Bonus Evaluation and Distribution Rules." The remuneration structure of managers are as follows: 1. Salary: Including salary, duty allowances, and severance pay. 2. Pension 3. Bonuses and special allowances 4. Employee remuneration amount: The amount of employee remuneration (including stock and cash) approved by the Board of Directors. If it is not possible to estimate, the proposed amount for this year will be calculated based on the proportion of last year's actual distribution.

Note 1: Since all directors of Giga Computing are directors or managers of its parent company, GIGABYTE Technology, and their remuneration is paid by GIGABYTE Technology, the directors' remuneration mentioned in this section is handled in accordance with the relevant provisions set forth in GIGABYTE Technology's "Articles of Incorporation."

3.2 Ethical Corporate Management and Legal Compliance

Item	Content
Policies, Commitments, and Importance	Ethical corporate management in operations and legal compliance are the foundation for establishing the Company's reputation and a strong brand image. They are also key to ensuring sustainable operations, reducing business risks, protecting stakeholder interests, enhancing employee job satisfaction and loyalty, and meeting regulatory standards and social expectations. We believe that only with this foundation can we become a true first-class enterprise. Giga Computing adheres to "Responsible Business Alliance (RBA) Code of Conduct" and the GIGABYTE Group's "Corporate Code of Conduct." These guidelines provide clear standards for aspects such as working conditions, company assets, and business activities. All commercial conduct must comply with legal requirements to protect overall societal interests and reduce environmental impact. To maintain the quality of business conduct, Giga Computing requires every new employee to sign the "Employee Code of Ethical Conduct". This document provides clear guidance and expectations regarding employees' values and behaviors, helping to establish an ethical, transparent, and responsible corporate culture.
Responsible Unit	General Manager's Office, General Administration Division
Action Plan	1. Commit to upholding the highest ethical standards, reflecting this commitment in all business activities, including but not limited to relationships with employees, customers, suppliers, industry peers, government, and the public (including shareholders). 2. Actively promote ethical corporate management by conducting advocacy for supervisors in each department, enhancing awareness and adherence to insider trading regulations and ethical policies among employees and management. Incorporate an "Employee Code of Ethical Conduct / Ethical Corporate Management" section into new employee training to ensure that every new employee completes relevant awareness education and learning upon onboarding. 3. If whistleblowing cases occur, continue to shorten the number of days required to close cases after receiving reports and increase the case closure rate. 4. In the future, the Company plans to distribute RBA Self-Assessment Questionnaires and Supplier Commitment Letters to key tier-one suppliers and to continue increasing the signing rate of Supplier Code of Conduct Declarations by suppliers with procurement amounts above a specified threshold.
2025 Performance	1. The signing rate of the "Employee Code of Ethical Conduct" statement by all employees was 100%. 2. At Giga Computing HQ, 100% of new hires completed anti-corruption training. Furthermore, anti-corruption and business integrity training is planned for all employees in 2026. 3. In 2025, no related reports were received.
Grievance Mechanism	In addition to actively promoting the importance of ethical corporate management and legal compliance among employees, Giga Computing also has multiple reporting channels, including the whistleblower mailbox and the HR mailbox. Upon receiving complaints, project-based management will be initiated, and appropriate actions will be taken based on the severity of the issue. We also commit that if compliance with regulations leads to commercial losses for the Company, no employees will be penalized or face adverse consequences as a result, in order to build a robust anti-corruption environment.

3.2.1 Anti-Corruption Communication and Training

To implement corporate ethics and ethical corporate management while facilitating the healthy development of corporate culture, Giga Computing adheres to the GIGABYTE Group's "Corporate Code of Conduct" and requires each new employee to sign the "Employee Code of Ethical Conduct." This provides clear guidance and expectations for employee values and behavior, helping to establish a culture of ethics, transparency, and responsibility. This approach aims to align the Company's internal goals with a consistent commitment to ethical corporate management. In 2025, 100% of Giga Computing's employees signed the "Employee Code of Ethical Conduct."In the future, we also plan to review the content of the declaration every three years in response to evolving trends or revisions to relevant standards and require employees to re-sign it, ensuring that employees continue to comply with the Company's ethical standards and ethical corporate management principles.

At the same time, to ensure that all employees are aware of anti-corruption measures and can effectively apply them in their daily operations, Giga Computing also implements education and training. Anti-corruption courses are integrated into new employee training to ensure every employee fully understands the Company's commitment to ethical corporate management, thereby protecting the quality of the Company's business practices. In 2025, 100% of new employees at Giga Computing HQ completed anti-corruption training.

To achieve subsequent targets, we will continue to plan and implement anti-corruption education for all employees to enhance professional ethics across the organization and fulfill our responsibilities to shareholders and to corporate social responsibility.

3.2.2 Ethical Corporate Management Policy

Ethical corporate management is one of the core values at Giga Computing and a fundamental principle that our employees must adhere to when performing their duties. We believe that only by adhering to this principle can we become a truly first-class enterprise. Giga Computing adheres to "Responsible Business Alliance (RBA) Code of Conduct" and the GIGABYTE Group's "Corporate Code of Conduct." These guidelines provide clear standards for aspects such as working conditions, company assets, and business activities. All commercial conduct must comply with legal requirements to protect overall societal interests and reduce external impact. To maintain the quality of business conduct, we prohibit all employees from engaging in any form of bribery, corruption, extortion, blackmail, embezzlement, or other unethical practices to achieve business objective. We also guarantee that if employee incurs potential business losses as a result of refusing to participate in or accept any these practices, the Company will not impose any punishment of adverse consequences, provided that the situation is verified. In addition to internal regulations, we also require key tier-one suppliers to sign and return the "Qualified Supplier Social Responsibility Management Commitment Letter" and plan to gradually increase the number of suppliers required to sign and return the "Commitment Letter" each year to ensure that key suppliers comply with relevant business ethics standards.

3.2.3 Whistleblower System

Giga Computing accepts reports of suspicious behavior through multiple channels and has established a dedicated whistleblower mailbox managed by a specialized internal auditor who reports directly to the Board of Directors. This allows internal and external parties to submit information about unlawful activities related to the Company and actively helps prevent fraudulent behavior. Upon receiving a report (including not submitted via the whistleblower mailbox, such as reports from the General Manager or the Board of Directors, written letters, or the HR Unit), the Board of Directors will assign a dedicated unit to form a project team based on the nature of the report. This team will investigate the suspected fraudulent activities described in the report. In 2025, the Company received no reports and will continue to establish relevant management measures as required by the Company's overall planning and regulatory requirements to enhance the reporting mechanism.

3.2.4 Legal Compliance

Compliance with regulations is a fundamental corporate responsibility and demonstrates a responsible attitude. Giga Computing upholds this principle, proactively monitoring regulatory changes and adjusting in a timely manner to meet the latest regulatory requirements. The Company has internal legal personnel and engages external lawyers and patent firms to provide legal and intellectual property services if required, to ensure that we comply with government regulations and administrative orders.

Giga Computing is committed to ensuring that all business activities comply with regulations of the countries and regions in which it operates, as well as with internal company rules and international standards. Additionally, we also regularly monitor regulatory trends and updates in various regions and adjust our internal operational standards and policies accordingly. Giga Computing expects employees to realize higher professional ethical standards when they are engaged in daily business, so as to maintain the Company's good reputation and become an excellent business partner.

Focusing on key regulations closely aligned with our business operations, the Legal & IP Affairs Division leads the coordination across all company departments to establish the following:

1. In alignment with the GIGABYTE Group, we establish systems for the dissemination, consultation, coordination, and communication of legal regulations as necessary, ensuring effective transmissions of legal requirements and the flow of information.
2. Regularly review and update various operational and management regulations, such as amending standard contracts, to comply with the requirements of relevant laws and regulations and ensure that the Company's operations comply with legal provisions.

From 2024 to 2025, Giga Computing did not encounter any incidents of violating regulations concerning product and service health and safety, environmental protection, product and service labeling/information, or marketing communications (including advertising, promotion, and sponsorship).

Note 1: A material violation is defined as a single incident resulting in cumulative fines of NT$1 million or more.

3.3 Risk Management

3.3.1 Risk Management Framework and Responsibilities

To enhance corporate governance and risk control capabilities, Giga Computing employs a layered management approach and establishes internal regulations to conduct risk assessments and management. This strategy aims to respond effectively to the ever-changing external environment, minimize risk impact, seize future development opportunities, and achieve sustainability goals.

■ **Risk Management Framework and Responsibilities**

Name of Organization	Scope of Responsibilities
Board of Directors	Ensure that major risks have been identified, determine the main strategic direction of material risks, and allow the organization to effectively control and reasonably allocate resources.
Senior Management	Implement the risk management policies formulated by the Board of Directors, coordinate cross-departmental risk management affairs, and track the risk management goals of each unit.
Audit Office	Audit daily risk management operations
Other Departments	Collect and execute daily risk management operations

3.3.2 Key Risks and Response Strategies

Giga Computing analyzes industry risk trends and holds risk management meetings with various departments to collect potential operational risks from different perspectives, classify risk factors, and take stock of the Company's current response strategies and status, ensuring that all potential risks remain within reasonable control and do not cause significant financial, reputational, or production impacts on the Company.

■ **2025 Risk Items and Future Response Strategies**

ESG Aspect	Governance				
Material Topics	**Corporate Governance**	**Moral Integrity and Code of Conduct**	**Information Security and Privacy Protection**	**Brand Strategy and Reputaition Management**	**Innovation Management**
Risk Factors and Descriptions	The absence of sound corporate governance mechanisms may lead to regulatory violations, failures in internal controls, and a decline in decision-making quality, thereby affecting the Company's reputation and operational stability.	The absence of relevant standards or management measures may increase risks such as corruption and misconduct, affecting the Company's operations and reputation.	There is a risk that sensitive data belonging to customers or the Company may be subject to external cyberattacks, ransomware, or data breaches.	Affect the Company's image and market trust, thereby reducing brand/corporate competitiveness and long-term value.	• Affect product competitiveness and technological development, thereby reducing market advantages. • The Company's reputation is affected by external infringement and competition.
Risk Management Policies	Hold ourselves to capital market standards, continuously strengthen the functions of the Board of Directors, and continually optimize the Company's governance mechanisms to ensure effective communication and coordination among relevant parties.	Adheres to "Responsible Business Alliance (RBA) Code of Conduct" and the GIGABYTE Group's "Code of Business Conduct." These guidelines provide clear standards for aspects such as working conditions, company assets, and business activities. All commercial conduct must comply with legal requirements to protect overall societal interests and reduce external impact.	Through the introduction of the ISO 27001 information security management system, we help the Company establish an information security management framework and establish an emergency information security incident reporting process to ensure that relevant incidents can be properly handled when they occur.	With "Compute for the Future" as our core corporate philosophy, we continue to strengthen brand identity and market positioning and provide high-quality server products and comprehensive solutions.	Established the Legal & IP Affairs Division to coordinate the Company's patent and trademark-related cases to protect the innovation achievements and intellectual property rights of colleagues and the Company.
Risk Response Strategies	**Ensure effective oversight:** Hold at least one Board of Directors meeting each quarter, including communication with the head of internal audit. **Performance evaluation mechanism:** Plan for the Board of Directors to establish performance evaluation criteria for directors and managers and regularly assess the achievement of their performance targets as a basis for remuneration.	**Establishing a culture of ethics:** Require all employees to sign the "Employee Code of Ethical Conduct" declaration and promote education and training related to ethical corporate management to ensure full understanding of and commitment to the Company's ethical standards, while integrating ethical corporate management and compliance requirements into operational processes and decision-making mechanisms and implementing them in daily business activities. **Establish grievance channels:** Set up a dedicated reporting mailbox managed by designated personnel to ensure that stakeholders can safely report concerns or irregularities; meanwhile, establish specific management targets for case closure days and case closure rates to improve handling efficiency and transparency and strengthen the effectiveness of the grievance mechanism.	**Information security incident management:** We have established rigorous information security incident classification system and clearly defined urgency of the incident. **Information security internal education and training:** Establish an internal information security education and training system and conduct phishing tests for all employees to enhance their ability to identify and respond to information security threats. **Management of confidential document rights:** Set up access levels for confidential company and customer documents to ensure that only personnel with appropriate authorization can access them.	**Strengthen brand image:** Strengthen the Brand's professional image and market trust through technical validation, successful case studies, and solution-oriented content. **Market research and customer insights:** Regularly conduct market trend analysis and customer needs research as a basis for product planning and marketing strategies. **Integrated marketing promotion:** Combine international trade shows, technical seminars, and digital marketing platforms, while introducing data analytics and CRM systems to enhance marketing precision and customer management effectiveness.	**Management Measures:** The Legal and Intellectual Property Office has established the intellectual property management process to effectively control the Company's internal patents and other related assets. **Encouragement of innovation:** Establish internal incentives for obtaining patents to encourage employees to continue pursuing innovation. **Resource investment, education and training:** Promote the effective implementation of innovation management through systematic planning and resource allocation, together with education and training on innovation-related topics.

ESG Aspect	Environment	Society		
Material Topics	GHG and Energy Management	Talent Recruitment and Retention	Talent Cultivation and Development	Occupational Safety and Health
Risk Factors and Descriptions	Operational losses or increased costs caused by extreme weather events or by climate change-related regulations enacted by countries, such as carbon fees and carbon taxes.	Loss of human resources due to the lack of adequate health and welfare benefits, comprehensive skills development, clear promotion pathways, and an equitable and inclusive workplace environment.	• A lack of clear career development paths may lead to talent loss, preventing investments in talent development from being effectively converted into organizational value. • Failure to establish a comprehensive succession plan and knowledge transfer mechanism may also lead to gaps in key talent, affecting operational stability and the organization's long-term competitiveness.	Failure to effectively implement relevant management measures may expose employees to various workplace hazards and increase the incidence of accidents, potentially resulting in occupational injuries or adverse health impacts, as well as risks such as business interruption, legal liability, and damage to corporate reputation.
Risk Management Policies	The Sustainability Promotion Team regularly conducts research and analysis on climate-related risks to understand the impact of climate change on the overall economic, environment and laws and regulations.	Establish a comprehensive job grade and remuneration system, complemented by well-developed welfare measures, to enhance overall employee well-being and job satisfaction, thereby promoting employee career development and the organization's stable growth.	Developed a talent cultivation blueprint based on comprehensive technological trends and the Company's future development direction. This blueprint establishes personnel development mechanisms and conducts soft-skills training in career development and workplace management, aiming to enhance corporate human capital.	Giga Computing has established management regulations such as the "Safety and Health Work Rules" and "Occupational Safety and Health Management Plan" to continuously improve workplace safety and health, reduce the risk of occupational accidents, protect employee safety, and promote employees' physical and mental well-being.
Risk Response Strategies	**Introduce the TCFD climate-related financial disclosure framework:** Since 2023, Giga Computing has benchmarked international standards, adopted the TCFD framework to assess and identify climate-related risks and opportunities, and established a climate governance framework and processes. **Voluntary GHG inventory:** Giga Computing conducts an annual voluntary GHG inventory of its operational scope in accordance with ISO 14064-1. In the future, based on the inventory results, subsequent reduction plans will be made to implement the Company's carbon management. **GHG inventory standard transition:** In 2026, the Company plans to transition from the current ISO 14064-1 GHG inventory standard to the GHG Protocol as the standard for conducting GHG inventories. **GHG assurance:** After completing the transition of the GHG inventory standard, the Company plans to obtain assurance on GHG inventory data in the same year to ensure and continuously improve the quality of relevant data.	**Establish a competitive remuneration system:** Determine remuneration based on job grade, education, work experience, years of service, and fair performance evaluation results, while ensuring internal equity and external competitiveness. In addition, establish diverse reward systems to motivate employees to improve performance and create value, thereby promoting the overall development of the organization. **Employee benefits:** Giga Computing has established a comprehensive employee benefits system, with dedicated units responsible for implementing group comprehensive insurance, daily health care, and family recreational activities to safeguard employees' health and well-being. **Employee satisfaction survey:** Conduct an anonymous online survey for all employees once a year, covering areas such as the work environment, management communication, welfare systems, and career development, and continuously enhance employee engagement and organizational trust through analysis of survey results and implementation of subsequent improvement measures.	**Talent cultivation:** We cultivate talents through on-the-job teaching, education and training, and the mentoring system to promote the effective learning and growth of our colleagues. **Education and training:** Reserve an annual budget for employee training to enhance employees' professional skills and leadership capabilities, and encourage employees to enrich themselves by participating in externally organized continuing education courses. **Key talent inventory:** Plan to launch a relevant program in 2026 to identify talent and capabilities that are critical to the Company's future growth and strengthen the completeness and stability of the overall talent pipeline.	**Hazard identification and risk assessment:** Identify and analyze occupational safety and health hazards related to chemical, physical, ergonomic, biological, and other safety and health factors to identify significant risks and implement corresponding control measures. **Education and training:** Plan and conduct occupational safety and health-related education and training based on factors such as regulatory requirements and potential workplace hazards to ensure that employees possess the necessary safety knowledge and risk identification capabilities, thereby reducing the likelihood of occupational accidents and enhancing overall workplace safety. **Health services and promotion activities:** Establish 4 major occupational health protection programs, continuously monitor employees' physical and mental health, and create a safe, healthy, and friendly workplace environment.

3.4 Information Security and Privacy Protection

Item	Content
Policies, Commitments, and Importance	1. In compliance with international information security standards (NIST CSF framework) and domestic and foreign information security regulations, the information security management regulations are reviewed and revised every year. 2. Ensure the confidentiality, integrity, and availability of information, so that information can be safely, correctly, appropriately, and reliably used to achieve the effectiveness of the planning, management, and execution of the business objectives. 3. To ensure a long-standing quality and safe product experience for customers, Giga Computing mandates that all aspects of the R&D process, product development, cloud services, and manufacturing supply chain adhere to information security policies. This approach aims to effectively reduce management risks and continuously enhance overall information security maturity. 4. Regularly conduct information security attack and defense drills and provide information security education and training to strengthen the information security awareness of internal employees and implement information security in every aspect.
Responsible Unit	General Manager's Office
Action Plan	1. Continue to implement information security education and training and social engineering drills to strengthen employees' information security awareness and vigilance, and to refine the information security framework for compliance and customer needs. 2. Occasionally perform vulnerability scans and penetration tests to prevent information security related risks. 3. In compliance with international information security standards (NIST CSF framework) and domestic and foreign information security regulations, we aim to implement information security and privacy protection with a more rigorous management approach. 4. The Information Security Promotion Committee holds a management review meeting every year to review and discuss matters related to the information security management system. 5. Conduct information security policy advocacy and education and training
2025 Performance	1. Conducted 4 social engineering drills and provided enhanced training courses for employees who did not pass. In 2025, the employee click-through rate for social engineering emails was 6%. 2. No major information security incidents occurred in 2025. 3. Obtained renewal of ISO/IEC 27001:2022 and CNS 27001:2023 information security management system certifications. 4. The information security risk and maturity level is maintained at Level A. 5. In 2025, the Company began conducting information security education and training for all employees, with a total of 2,195 attendees. The completion rate for information security education and training for all employees was 88.79%. 6. Establish supply chain information security risk management regulations and conduct supply chain information security assessment briefing sessions.
Grievance Mechanism	Giga Computing's Privacy Policy

3.4.1 Information Security Policy

At Giga Computing HQ, the Information Technology Division is responsible for implementing information security policies, conducting risk assessments, promoting and tracking various response measures, and regularly reporting on the implementation status to senior management. Through the implementation of the ISO 27001 information security management system, establish a systematic management mechanism to ensure the proper protection of information assets.

1. In compliance with international information security standards (NIST CSF framework) and domestic and foreign information security regulations, the information security management regulations are reviewed and revised every year.
2. Ensure the confidentiality, integrity, and availability of information.
3. Supply chain information security management must comply with the information security policy.
4. Regularly conduct information security attack and defense drills to strengthen the information security awareness of internal employees.

Giga Computing has also established privacy policy regulations applicable to the Company's overall operations and ensures that all risk treatment measures comply with the Company's security policies and procedures. As part of compliance reviews, regularly review and update the privacy policy to ensure alignment with relevant laws and regulations, comply with the latest regulatory requirements, and refer to industry best practices such as the GDPR and CCPA, continuously incorporating them into the privacy policy.

3.4.2 Responsible Unit for Information Security

To effectively promote and carry out information security initiatives, Giga Computing HQ has established the Information Security Promotion Committee, which is responsible for formulating information security strategies, reviewing management systems, planning the overall direction of development, and overseeing the effectiveness of the information security management system. The Information Security Promotion Committee holds a management review meeting at least once a year and may convene extraordinary meetings when necessary to ensure the continued effective operation of the system.

Through the division of responsibilities between the Information Security Promotion Committee and the Information Management Division, Giga Computing HQ has established a comprehensive information security governance framework that integrates strategic planning with effective implementation to strengthen overall information security management.

Responsible Unit

Information Security Promotion Committee: Oversee the initial review, promotion, and coordination of information security policies, management systems, plans, and related tasks.

- Convener: Handle and supervise information security related operations.
- Deputy Convener: Assist the convener in handling and supervising information security related operations.
- Information Security Implementation Team: The committee has established an Information Security Implementation Team to handle administrative and technical aspects of information security management.
- Information Security Audit Team: The committee has established an Information Security Audit Team to conduct audits of information security management.
- Emergency Response Team: The committee may form an Emergency Response Team to handle information security emergencies.

3.4.3 Information Security Risk Assessment

To maintain information security risk and maturity at Grade A, an information security maturity assessment is conducted annually using quantitative indicators to evaluate areas such as the implementation of information security policies, risk management mechanisms, the extent of technology application, employee information security awareness, and supply chain information security protection, thereby reviewing the effectiveness of the Company's information security management system and identifying directions for continuous improvement. Giga Computing HQ established information asset risk assessment standards to identify the vulnerabilities and threats to information assets, and based on the assessment results, implement countermeasures or control measures to reduce the risk of damage to information assets.

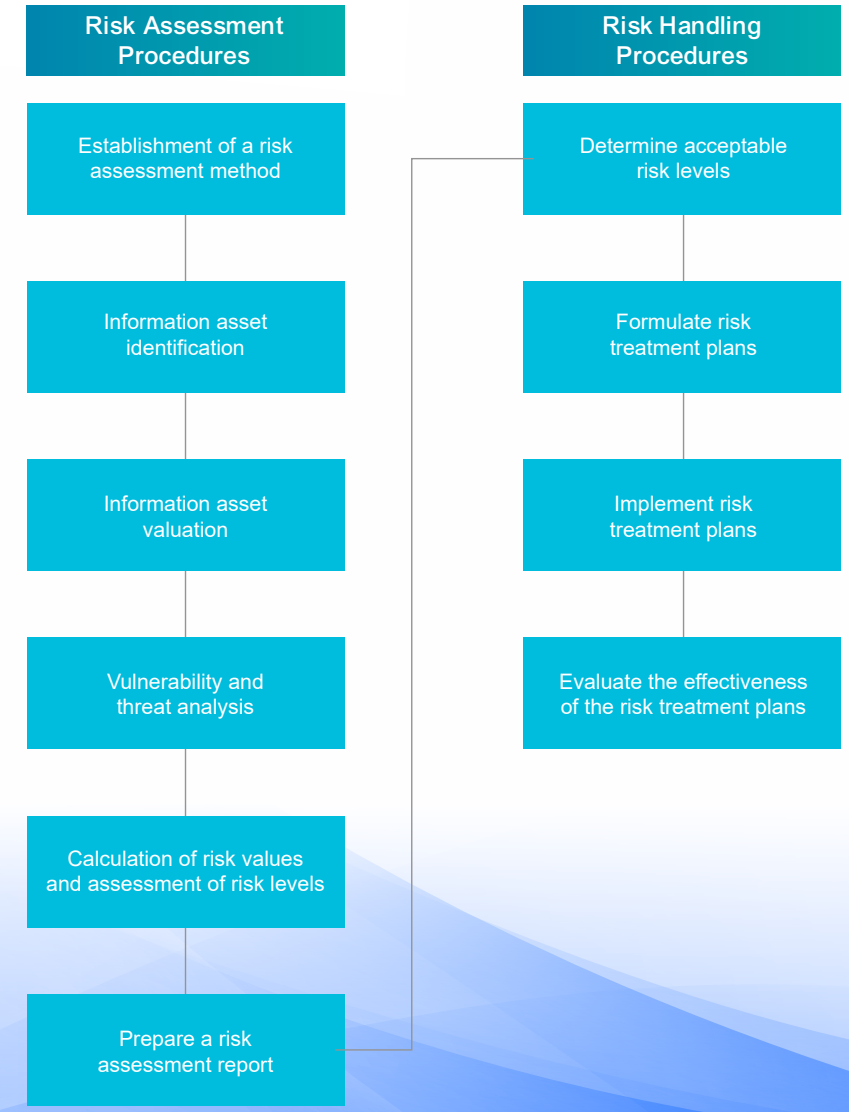
Information Security Implementation Team

1. Establish and maintain systematic risk assessment methods
2. Supervising the execution of risk assessments
3. Determine the acceptable risk level
4. Review the risk treatment plan and confirm the implementation effectiveness
5. Determine the timing and scope of risk assessments.
6. Prepare the risk assessment report and submit it to the Information Security Promotion Committee
7. Prepare the risk handling plan and submit it to the Information Security Promotion Committee

Information Asset Manager

1. Implement risk assessment operations
2. Formulate the risk assessment report
3. Formulate and implement risk treatment plans

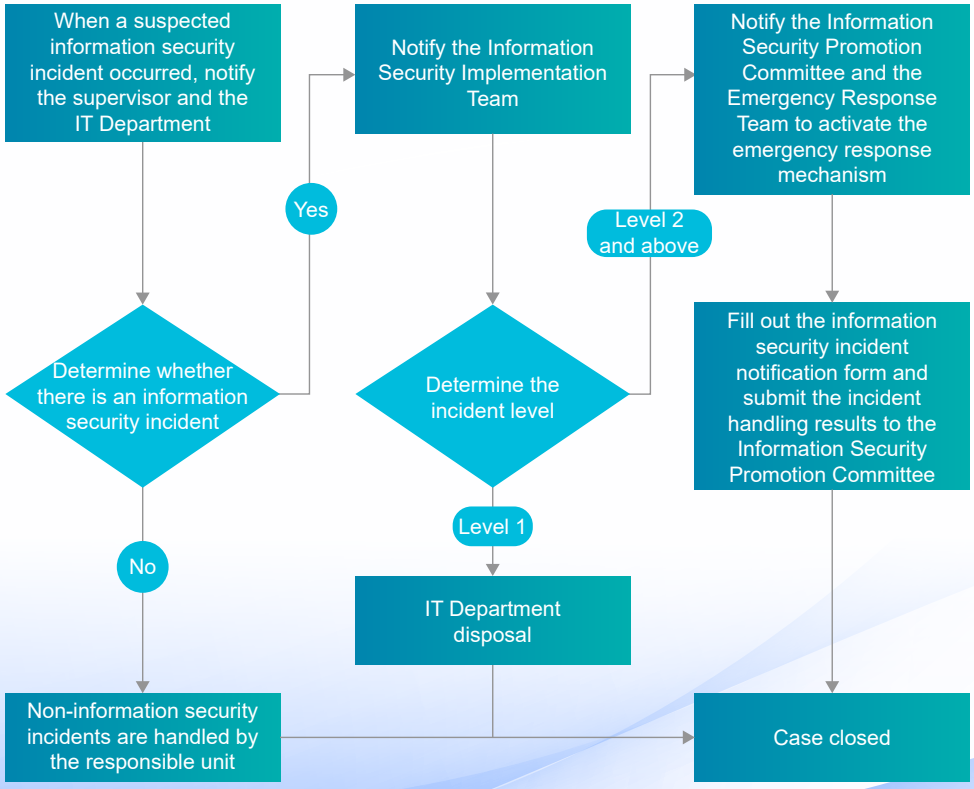
Risk management refers to the risk control process for information assets that includes the "Risk Assessment Procedures" and "Risk Handling Procedures." The main operating items are shown in the figure below:



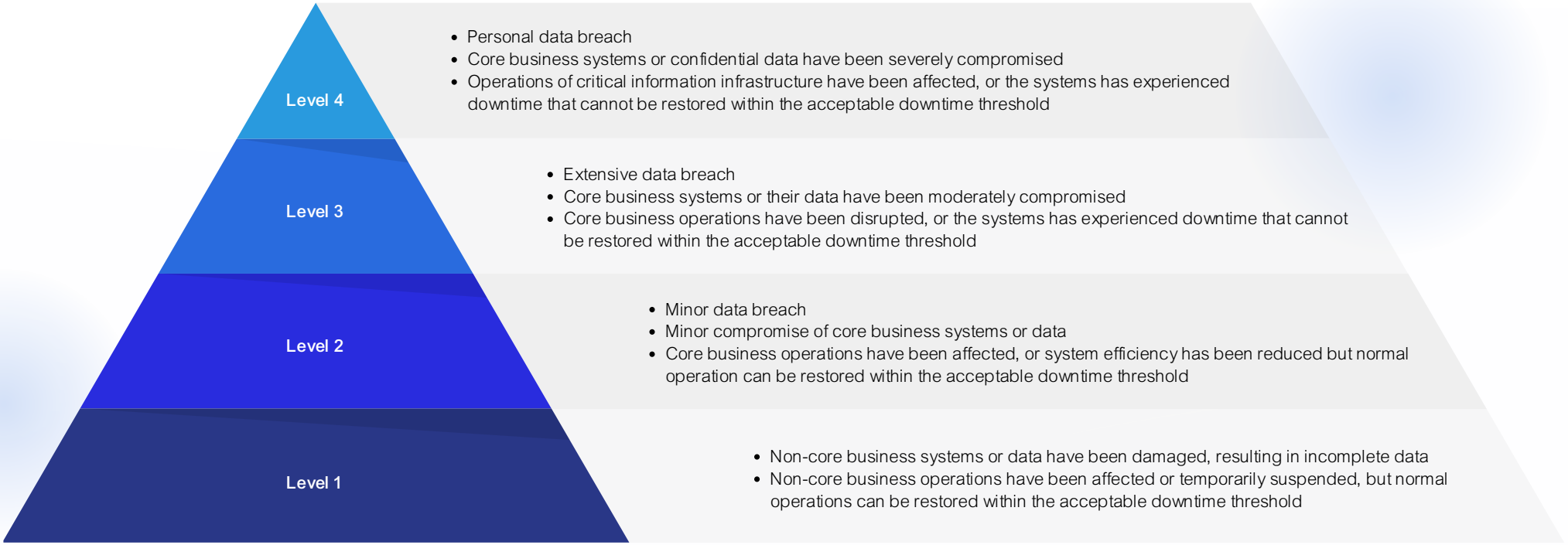
3.4.4 Procedures for Reporting Information Security Incidents

In the event of a suspected information security incident, the discoverer must report it to the responsible authority and inform their direct supervisor. After receiving the notice, the direct supervisor will evaluate whether it is an information security incident. If the incident is determined to be a non-information security incident, the supervisor will notify the discoverer. If the incident is determined to be an information security incident, an initial estimate of the handling time will be made and the Information Security Implementation Team will be notified to assess whether to activate the Emergency Response Tam operations.

In the event of an information security incident, the Information Technology Division should record the following details, including the facts of the incident, the potential impact, loss assessment, assessment for support needs, and the measures taken in response.



Classification of Information Security Incidents



To strengthen the response to and management of information security incidents, Giga Computing HQ has established a tiered reporting and handling mechanism for such incidents. Incidents are managed according to their level of impact, with clear reporting procedures and divisions of responsibility to ensure timely responses and reduce potential effects when incidents occur.

When an information security incident occurs, the relevant information security units will coordinate resources and response operations, while other relevant units will assess and handle the incident in accordance with the tiered mechanism and activate a cross-departmental response mechanism when necessary. If external communication is required, the head of the Emergency Response Team must report to the Chief Information Officer and assist Giga Computing's spokesperson in explaining the situation and response measures to external parties.

In 2025, Giga Computing did not experience any major information security incidents classified as "Level 4" or above.

3.4.5 Response Strategies for Information Security

Information Security Incident Response Process

To prevent interruptions in data center operations, Giga Computing HQ protects critical business processes from major failures or disasters by formulating alternative plans that can be executed when such processes are affected. This approach ensures employee safety and business continuity, reduces losses caused by incidents, and serves as the basis for the development and maintenance of the business continuity plan. The impact and severity of each business service process are assessed to determine the Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO), and Recovery Point Objective (RPO); based on the importance of each process, a criticality level of "high," "medium," or "low" is assigned. Processes classified as "high" criticality are identified as our critical business processes. The Information Security Implementation Team is responsible for reviewing plan changes. The business continuity plan shall be reviewed and evaluated at least once a year, including conducting business impact analysis, adjusting organizational responsibilities and membership, reviewing disaster response procedures and recovery strategies, and reporting the results of the annual comprehensive review and updates to the Information Security Promotion Committee.

Enhance Employees' Information Security Risk Awareness

Giga Computing arranges information security education and training annually according to the business duties and roles of different positions. Information security dedicated personnel in the IT Department must receive at least 2 hours of information security education and training each year; new employees receive relevant information security education and training from the HR Department to ensure they understand the Company's information security management requirements. In 2025, the Company began conducting information security education and training for all employees to enhance employees' information security risk awareness and reduce the occurrence of information security-related risk incidents. A total of 2,195 attendees were recorded, with a completion rate of 88.79%. The Company aims to maintain a completion rate of over 80% in 2026 and achieve a completion rate over 90% by 2030.

To enhance employees' awareness of information security, the Information Security Implementation Team uses the internal website or email each year to inform employees of the latest information security threats and help prevent risks. In 2025, a total of 4 employee social engineering email exercises were conducted, with a click-through rate of 6%, meeting the 2025 target of less than 20%. At the same time, to address information security-related risks, starting in 2026, Giga Computing HQ will adopt a more stringent target and continue to conduct relevant education, training, and awareness activities with the aim of achieving a social engineering click-through rate of less than 10%.

In addition to the above measures, Giga Computing HQ requires employees to comply with relevant security regulations when entering or leaving office and data center environments. Furthermore, employees must adhere to applicable laws and regulations while performing their duties. Any violations (such as the disclosure of confidential information via computers and the theft of personal data) will be subject to disciplinary action in accordance with the Work Rules, depending on the severity of the circumstances, thereby reducing the likelihood of information security incidents.

Course Title	Form of Handling	Participants	Number of People Trained	Course Hours	Total Trainin Hours
Information security education and training	Physical	Information security personnel in the IT Department	4	2 hours	8 hours
Information security awareness education and training	Physical	New employees	185	10 minutes	30.83 hours
Targeted Social Engineering Remedial Training	Online	Employees who failed the drill	80	30 minutes	40 hours
Information security education and training for all employees -1/3	Online	All employees	610	1 hours	610 hours
Information security education and training for all employees -2/3	Online	All employees	682	1 hours	682 hours
Information security education and training for all employees -3/3	Online	All employees	657	1 hours	657 hours
Supply Chain Information Security Assessment Briefing	Online	Supplier	73	1 hours	73 hours
Total					2,100.83 hours

Note 1: The data and information in this table cover Giga Computing HQ.