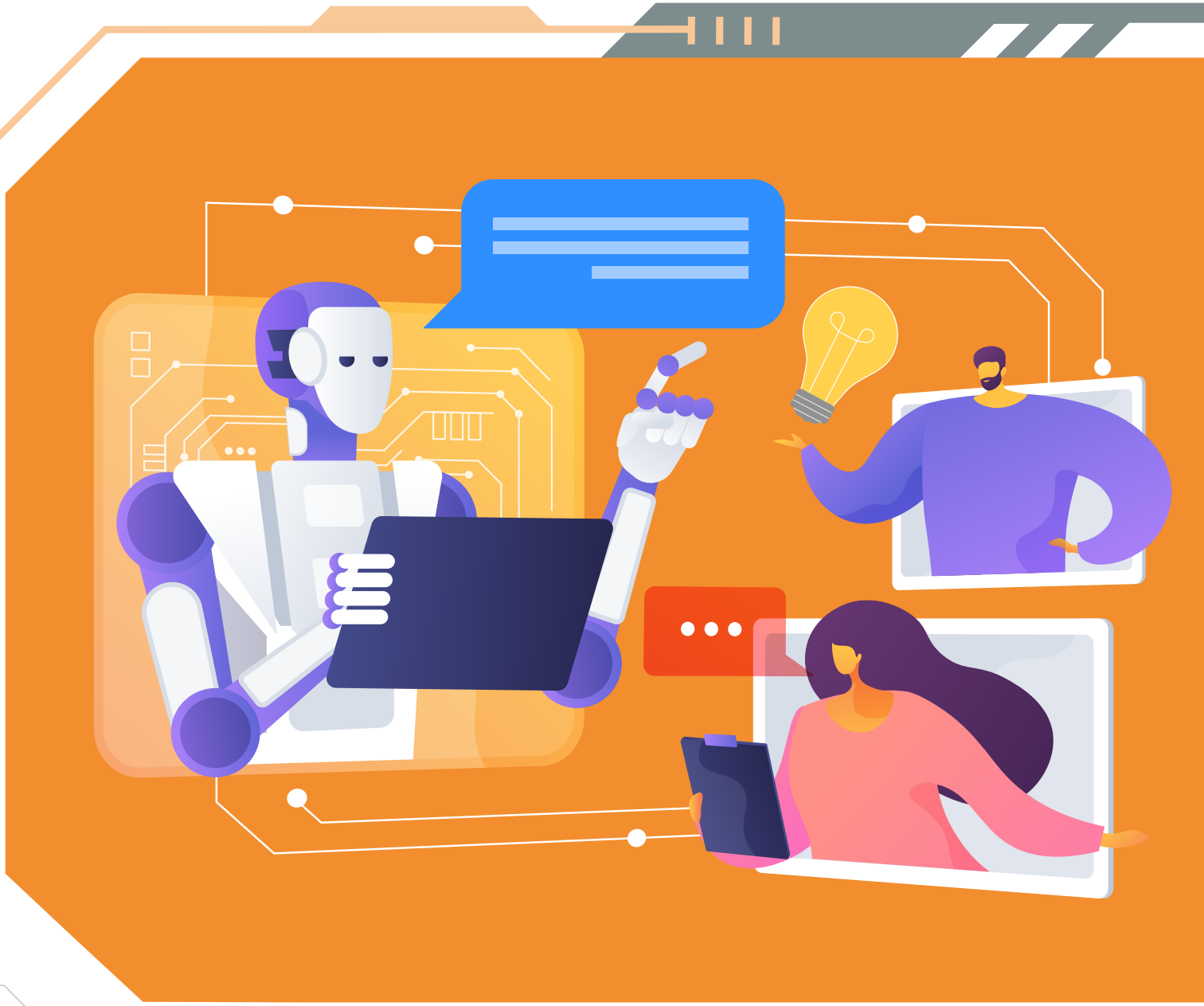
3

Corporate Stable Operations



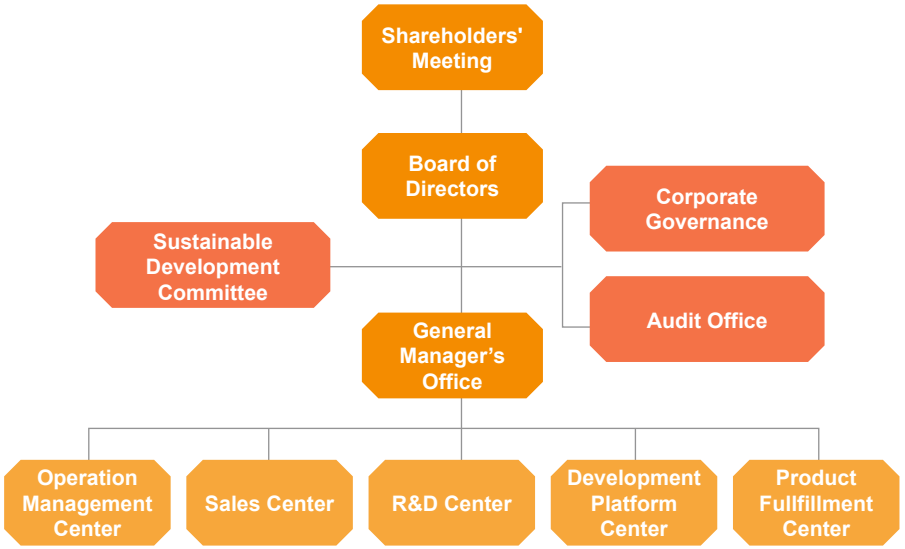
3.1 Corporate Governance

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. The Board of Directors is responsible for establishing performance evaluation standards for directors and managers and regularly assessing the achievement of their performance goals. These evaluations serve as the basis for determining individual remunerations.
2024 Performance	1. Establish an independent audit unit to supervise the Company's various operating activities through the internal audit mechanism. 2. 7 Board of Directors' meetings were held during the year, with an average attendance rate of 82.86%. 3. The average number of training hours per director is 7.20 hours. In the future, the directors will continue to take appropriate courses based on the needs of the market and governance.
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 2024, the average attendance rate of the Board of Directors' meeting was 82.86%.

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, a Corporate Governance Unit, and an 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 2024. 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 7.20 hours of continuing education.

2024 Continuing Education of Directors

Course Offering Unit	Course Title	Course Hours (hours)	Number of Trainees	Training Hours (hours)
Accounting Research and Development Foundation	How the Board Oversees Corporate Risk Management and Crisis Handling	3	4	12
	How the Board Ensures Corporate Sustainability—From Talent Discovery to Development	3	4	12
	Common Deficiencies in Financial Statement Reviews and Common Issues in Asset Acquisitions/Disposals	3	1	3
	Effective Internal Control for Sustainability Reporting	3	1	3
	Strengthening Internal Control Functions and Board Operation Mechanisms with Fraud Case Studies	6	1	6
Total Training Hours		36 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	2022.03.08	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	2022.03.08	3 years	Master of Computer Engineering of California State University (CSU), Chico	Director of GIGABYTE Technology General Manager of GIGABYTE Technology Chairman of GIGAIPC Co., Ltd. Director Representative of Giga-Trend International Investment Group Ltd. Director Representative of MyelinTek Inc. Independent Director of PCL Technologies, Inc.
Director	Yang Hsueh-Ching	Female	61-70	2024.09.02	3 years	National Taipei University of Business	Director 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	2022.03.08	3 years	Electronic and Computer Engineering, National Taiwan University of Science and Technology	Director 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	2022.03.08	3 years	Minghsin University of Science and Technology	Director 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-Cheng, 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 2024, 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 2024. 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.

Remuneration Policy

Directors	Managers
The directors' remuneration at the Company is allocated according to the provision of the GIGABYTE Group's "Articles of Incorporation," 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 GIGABYTE Group'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: The amount of various bonuses, incentives, transportation fees, special allowances, various subsidies, dormitories, company vehicles, and other forms of remuneration for the most recent fiscal year. 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.

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 Administrative 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.
2024 Performance	1. The signing rate of the "Employee Code of Ethical Conduct" statement by all employees was 100%. 2. The proportion of new employees at Giga Computing HQ receiving anti-corruption training is 51.37%. Moving forward, we will continue to strengthen this training and plan to implement anti-corruption and ethical corporate management training for all employees. 3. In 2024, 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 a whistleblower mailbox and a 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 2024, 100% of Giga Computing's employees signed the "Employee Code of Ethical Conduct."

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 2024, at Giga Computing HQ, 51.37% of new employees received anti-corruption training, with a total of 94 employees completing the training.

To achieve subsequent targets, we adjusted the anti-corruption training approach for new employees in 2025 to effectively increase the proportion receiving training. Moving forward, 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 2024, Giga Computing did not receive any reports on ethical and integrity standards. Moving forward, the Company will establish relevant evaluation mechanisms before establishing business relationships with suppliers, customers, and other business partners, taking into account the Company's actual operational needs.

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, 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 2024, 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.

We focus on important laws and regulations closely related to our operations, and establish the following matters with each department:

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.

In 2024, Giga Computing did not encounter any incidents of violating regulations related to the health and safety of products and services, environmental regulations, product and service information, or marketing (including advertising, promotions, and sponsorships).

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.

Giga Computing's 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. In 2024, Giga Computing identified the following major operational risks, including financial risks, information security risks, supply chain risks, innovation and intellectual property risks, climate change risks, and human resource risks. The table below outlines the Company's management policies, procedures, and response strategies for addressing these risks.

2024 Risk Items and Future Response Strategies

ESG Aspect	Governance	Governance	Governance	Governance	Environment	Society
Risk Items	Financial risk	Information security risk	Supply chain risk	Innovation and intellectual property risk	Climate change risk	Human resource risk
Risk factors	Market risk, price risk, credit risk and liquidity risk.	The risk of extortion or leakage of sensitive data of customers or the Company by external hackers.	Issues such as supply chain disruptions and material shortages caused by geopolitical factors or internal defects of suppliers, or potential violations of human rights and CSR by suppliers, which could negatively impact the Company's image.	The Company's reputation is affected by external infringement and competition.	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.

ESG Aspect	Governance	Governance	Governance	Governance	Environment	Society
Risk Items	**Financial risk**	**Information security risk**	**Supply chain risk**	**Innovation and intellectual property risk**	**Climate change risk**	**Human resource risk**
Risk Management Policies and Procedures	The Finance Department works closely with the operating units to identify, assess, and manage financial risks to ensure risk mitigation and appropriate control.	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.	Giga Computing follows the "GIGABYTE Sustainable Procurement Guidelines" and, referencing the "RBA Code of Conduct," establishes 4 major suppliers management aspects, 15 sub-targets, and 4 zero-tolerance regulations to comprehensively manage suppliers and proactively prevent risks.	Giga Computing has established the Legal and Intellectual Property 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.	Giga Computing's 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. In the future, we will further improve the relevant risk management policies and procedures to cope with these changes.	1. Ensure that employee safety, salaries and benefits, and workplace environment comply with relevant regulations to safeguard employee well-being, and adopt corporate policies that appropriately exceed regulatory requirements to mitigate human resource-related risks. 2. 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 training in career development and workplace management, aiming to enhance corporate human capital.
Risk Response Strategies	**Market Risk (Price Risk):** Giga Computing adopts an investment portfolio diversification strategy, making investments based on set limits to effectively control market risk. **Credit Risk:** According to clearly defined internal credit policies, perform management and credit risk analysis for each new customer before finalizing payment and delivery terms. Evaluate customers' credit quality by considering their financial situation, past experience, and other factors. **Liquidity Risk:** When holding excess cash beyond operational needs, reallocate it back to the Finance Department. The Finance Department then manages liquidity risk by adjusting and forecasting based on funding requirements.	**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.	**Supplier Audit:** Regularly audit high-risk suppliers and new suppliers, and eliminate inappropriate suppliers as necessary. **Implement Local Procurement:** Continue to implement local procurement to reduce the risks that may occur during long-distance transportation. **Conflict Minerals Management:** Investigate the use of conflict minerals with first-tier suppliers every year to prevent the use of conflict minerals in products.	**Management Measures:** The Legal and Intellectual Property Affairs Division has established the intellectual property management process to effectively control the Company's internal patents and other related assets. **Encouragement of Innovation:** Giga Computing offers internal rewards for obtaining patents and additional bonuses for researching and developing energy-saving or green products to incentivize employees to continue innovating.	**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.	**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. **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.

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.
2024 Performance	1. Employee social engineering email click rate: 23.33%. 2. No major information security incidents occurred. 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. Establish supply chain information security management guidelines and incorporate them into supplier management processes. 6. Conducted one social engineering drill and provided enhanced training courses for employees who did not pass. 7. Conduct information security policy advocacy and education and training.
Grievance Mechanism	Giga Computing's Privacy Policy

3.4.1 Information Security Policy

The Information Technology Division is responsible for formulating information security policies, risk assessment, and implementation and follow-up of countermeasures. The CIO reports the implementation status to the General Manager occasionally every year. In order to reduce the risk of non-compliance and increase customer trust, we have also introduced the ISO 27001 information security management system to establish a comprehensive and systematic approach to managing and protecting the Company's 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.

3.4.2 Responsible Unit for Information Security

To effectively promote and manage all aspects of information security within the management system at Giga Computing, an Information Security Promotion Committee has been established. This committee is responsible for formulating the direction, strategies, and steps for information security development, ensuring the continuous and stable operation of the information security management system. The Information Security Promotion Committee shall convene a management review meeting at least once a year, and may convene an extraordinary meeting when necessary.

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 at Giga Computing.
- **Deputy Convener:** Assist the convener in handling and supervising information security-related operations at Giga Computing.
- **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

Giga Computing 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.

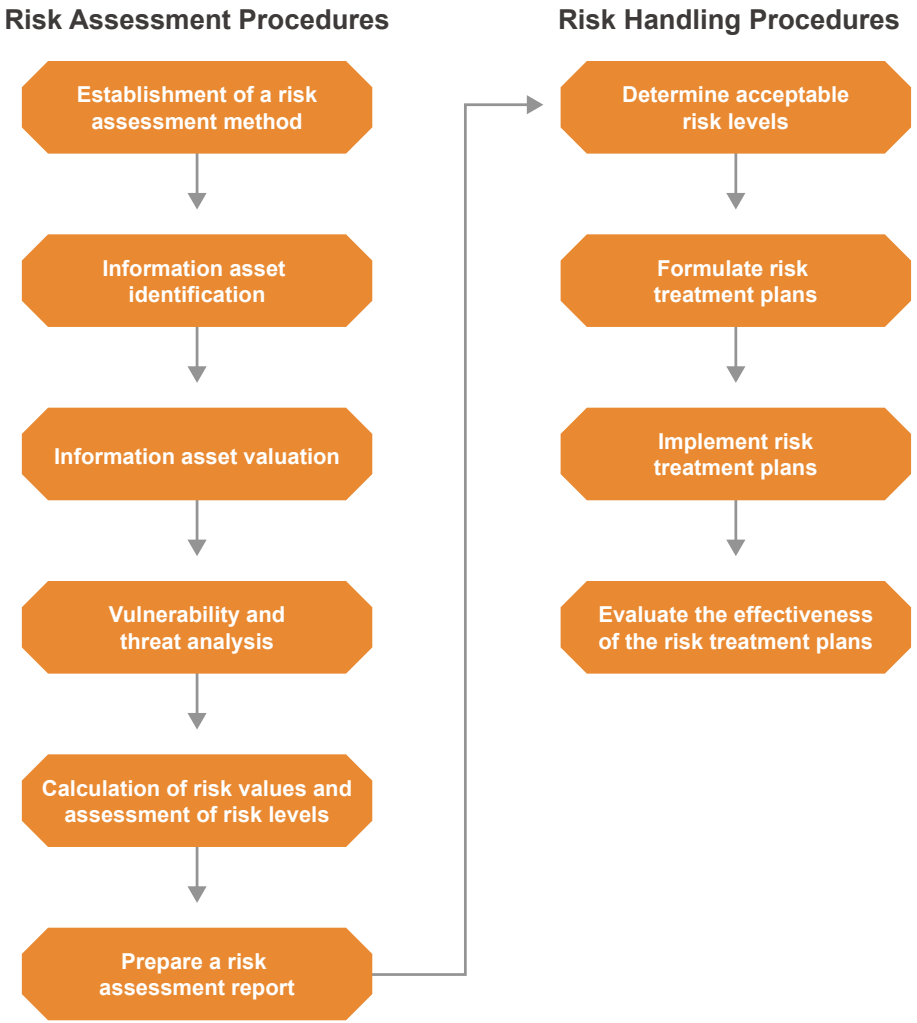
Information Security Implementation Team

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 management plans.

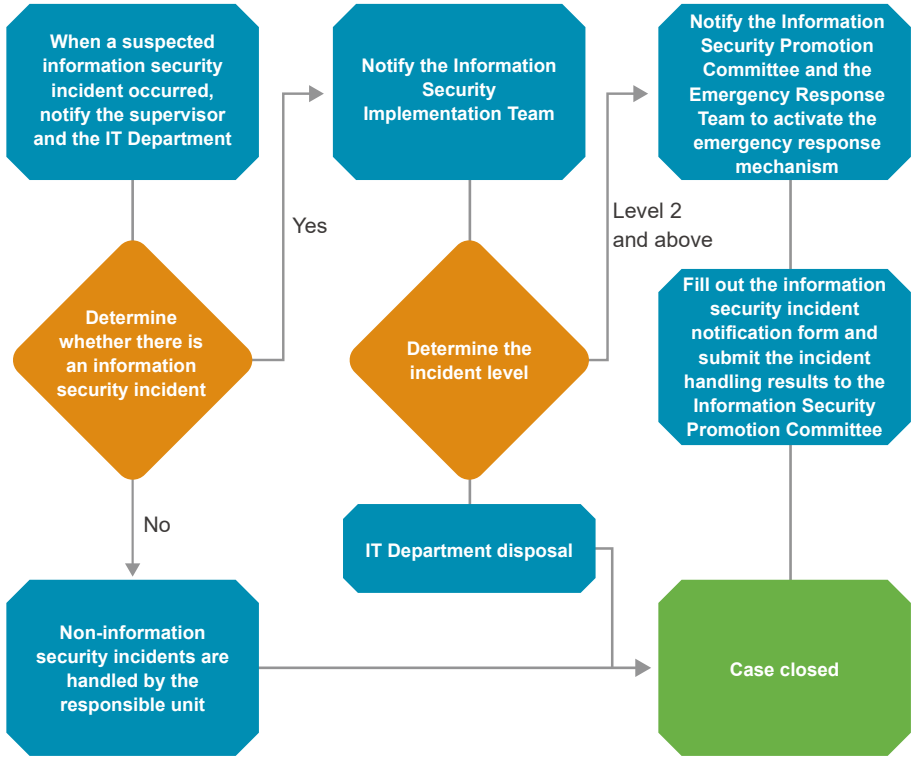
Risk management refers to the risk control process for information assets that includes the "Risk Assessment Procedures" and "Risk Handling Procedures." The main operating items are shown in the figure below:



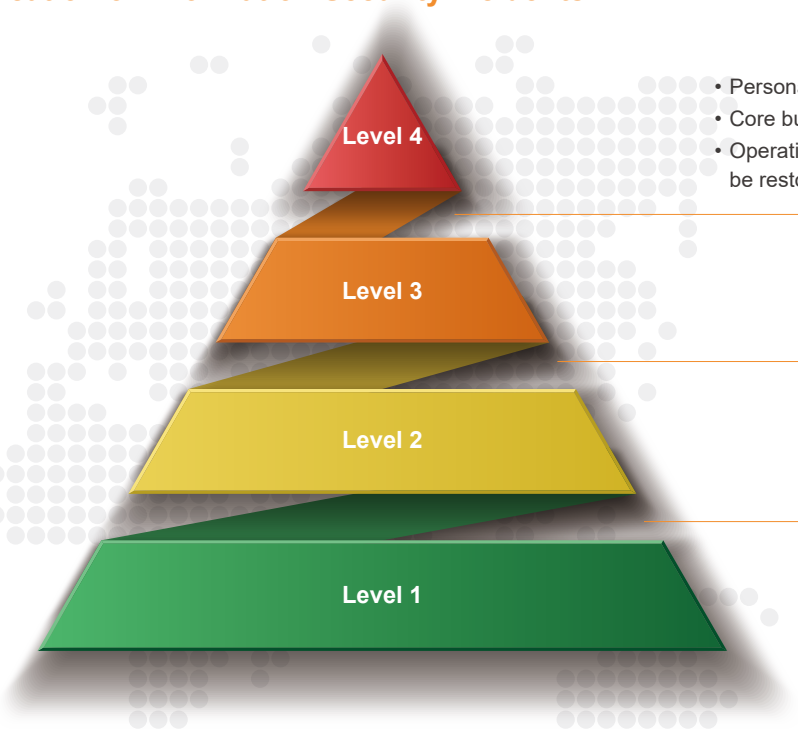
3.4.4 Procedures for Reporting Information Security Incidents

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



Level 4
- Personal data breach.
- Core business systems or confidential data have been severely compromised.
- Operations of critical information infrastructure have been affected, or the systems has experienced downtime that cannot be restored within the acceptable downtime threshold.

Level 3
- Extensive data breach.
- Core business systems or their data have been moderately compromised.
- Core business operations have been disrupted, or the systems has experienced downtime that cannot be restored within the acceptable downtime threshold.

Level 2
- Minor data breach.
- Minor compromise of core business systems or data.
- Core business operations have been affected, or system efficiency has been reduced but normal operation can be restored within the acceptable downtime threshold.

Level 1
- Non-core business systems or data have been damaged, resulting in incomplete data.
- Non-core business operations have been affected or temporarily suspended, but normal operations can be restored within the acceptable downtime threshold.

3.4.5 Response Strategies for Information Security

To prevent interruptions in data center operations, Giga Computing 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 Giga Computing's 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.

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. The Information Security Implementation Team uses the internal website and emails to inform staff about the latest security threats and to prevent risks. In 2024, the employee social engineering email click rate was 23.33%. Starting in 2025, we have set a target click rate of less than 20% and plan to use company-wide information security training to enhance employee risk awareness and reduce incidents related to information security.

Information Security Education and Training Hours

Course Title	Course Topic	Form of Handling	Participants	Number of People Trained	Course Hours	Total Training Hours
Information security education and training	ISO 27001 Awareness and Audit Response Techniques, 2024 Information Security Updates	Physical	Information Security Personnel in the IT Department	4	2 hours	8 hours
Information security awareness education and training	Promote the Company's information security policy and strengthen security awareness	Physical	New employees	141	10 minutes	23.5 hours
Intensive social engineering drill	Enhance safety awareness and vigilance	Online	Employees who failed the drill	100	30 minutes	50 hours
Total				**245**	**-**	**81.5 hours**

Employees entering or leaving office areas and data centers shall comply with relevant security regulations; they shall comply with relevant laws and regulations when performing their duties. If there is any violation (such as computer leakage, and personal data theft), they will be punished according to the work rules depending on the severity.

1. When the incident has a lower impact and minor consequences, involving only internal units and causing slight damage (such as internal security issues, computer virus infections), and the unit involved determines the security incident level as "Level 1," the unit will handle it on its own and notify the unit supervisor of the situation after resolution.
2. If the unit involved in the security incident determines the incident level to be "Level 2" or higher, it should immediately report to the Information Security Implementation Team. The team will then analyze and identify the incident, consolidate information, and notify the Information Security Promotion Committee convener, who will decide whether to activate the emergency response mechanism.
3. In the event of a security incident, the head of the Emergency Response Team should be responsible for contacting the team, coordinating and supervising the execution of tasks by the key business process owners, and managing the allocation of resources.
4. If the security incident level reaches "Level 2" or above, the unit where the incident occurred and the Information Security Implementation Team should complete the "Information Security Incident Notification Form" and submit the incident handling results to the Information Security Promotion Committee.

When handling information security incidents, the Information Security Promotion Committee is responsible for integrating company resources and providing necessary assistance as needed. When an information security incident requires external communication, the head of the Emergency Response Team must report to the CIO and assist the spokesperson of Giga Computing in explaining the situation and the response measures to the public. In 2024, Giga Computing did not experience any major information security incidents classified as "Level 4" or above.