2

Corporate Stable Operations

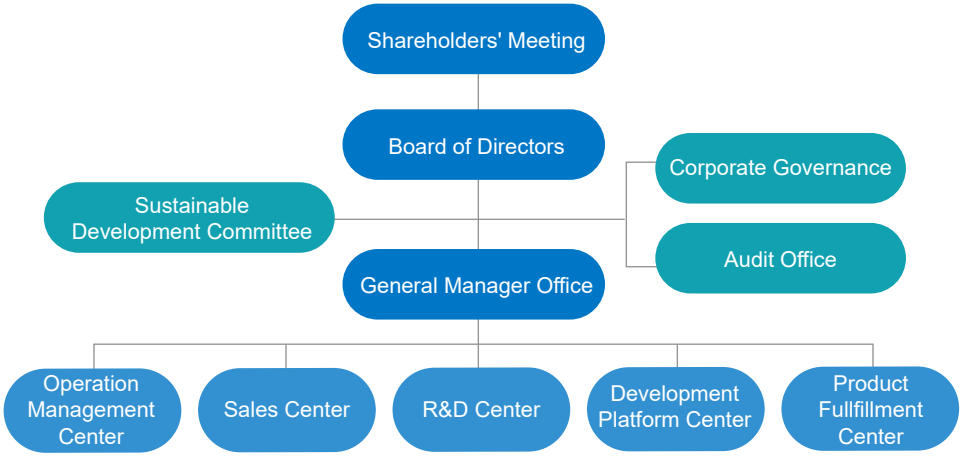
2.1 Corporate Governance

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 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 Office, Finance & Accounting Division
Short-, Mid-, and Long-term Goals	**Short-term goals (2024):** 1. Aligning with regulatory standards and timelines, the Company will carry its governance planning. **Mid- and long-term goals (2025-2030):** 1. Strengthen the functions and improve the corporate governance capability of the Board. 2. Improve the sustainability governance structure, promote the setting of internal ESG goals, and drive internal transformation with goals. 3. Implement corporate governance evaluations and actively communicate with stakeholders to continuously deepen the Company's culture of sustainable governance.
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 meetings, and the audit plan for the following year shall be approved at the end of the year. 2. The Board 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.
2023 Performance	1. Establish an independent audit unit and supervise the Company's various operating activities through the internal audit mechanism. 2. In 2023, the average attendance rate of the board meetings was 80%. 3. The average number of training hours per director is 6.6 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 information of the Company are also occasionally announced on the official website and published on the MOPS as required by the Company Act.

2.1.1 Corporate Governance Structure

The Board is the highest governing body of the Company, which consists of 1 Chairman, who serves as the head of the Board internally and represents the Company externally. In addition to fulfilling its responsibilities as stipulated by laws, regulations, and shareholders' resolutions, the Board has the authority to oversee the Company's annual and semi-annual financial reports, evaluate the effectiveness of the internal control system, and appoint or dismiss CPAs. The Board must also approve appointments, dismissals, and strategic plans to ensure that the Company's long-term development aligns with its vision and values. In 2023, the average attendance rate of the board meetings was 80%.

The General Manager, entrusted with responsibilities by the Board, 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, in 2023, we planned the establishment of a 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 2023. Moving forward, we will gradually initiate the functions of these governance units according to the Company's plan, aiming to strengthen the governance mechanisms.



2.1.2 Board Diversity and Continuing Education

The Company follows a board diversity policy to ensure effective corporate governance, enhance the functions of the Board, and improve the Board's structure. The board has established appropriate background diversity policies based on the Company's operational model and needs, leading to a progressively diversified selection of board members. Through diverse recruitment experiences, we have attracted talent with varied professional backgrounds, skills, and industry experience, continually enhancing corporate governance and operational synergies.

The Company's current board consists of 5 members, aged between 51 and 70, with expertise in business, technology, and industry marketing. Each director brings extensive experience in their respective industries. In the future, to continue promoting the sound development of the Board's composition and structure, Giga Computing will persist in implementing the board diversity policy to enhance corporate governance effectiveness and management performance.

The Company encourages board members to pursue continuous education to enhance their professional skills and knowledge, stay updated on current industry trends 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, the board members participated in training courses, with an average of 6.6 hours of continuing education.

◆ 2023 Continuing Education of Directors

Course Offering Unit	Course Title	Training Hours (hours)
Accounting Research and Development Foundation	Operation diversification strategy under geopolitical risks	3 hours*5 directors
Accounting Research and Development Foundation	Fiscal and taxation thinking of taiwanese businesses under the trend of global re-arrangement of supply chain	3 hours*5 directors
Taiwan Corporate Governance Association	Anti-tax avoidance wave—CFC responses and new M&A ideas that taiwanese businesses need to know	3 hours*1 director
Total Training Hours	33 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 to 70	2022.03.08	3 years	EMBA, National Chengchi University Minghsin University of Science and Technology	Chairman of GIGABYTE Chairman of Giga Investment Corp. Chairman of Giga-Byte Communications Inc. Director Representative of G-Style Chairman of Giga-Trend International Investment Group Ltd. Chairman of PG Union 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	51 to 60	2022.03.08	3 years	California State University (CSU), Chico Master of Computer Engineering	Director Representative of GIGABYTE Chairman of Gigiaipc Co., Ltd. Director Representative of MyelinTek Inc.	
Director	Liu, Ming-Hsiung	Male	61 to 70	2022.03.08	3 years	EMBA, National Chengchi University	Vice Chairman of GIGABYTE Director Representative of Giga Investment Corp. Director Representative of Giga-Byte Communications Inc. Chairman of G-Style Director of Info-Tek Corporation Director Representative of Giga-Trend International Investment Group Ltd. Supervisor Representative of Hui Yang Venture Capital Co., Ltd.	Supervisor Representative of BYTE International Co., Ltd. Director Representative of JM Material Technology Inc. Supervisor Representative of Senyun Precise Optical Co., Ltd. Director Representative of Yuncheng Ltd. Supervisor Representative of AMIDA Technology Inc.
Director	Ma, Mou-Ming	Male	61 to 70	2022.03.08	3 years	Electronic & Computer Engineering, National Taiwan University of Science and Technology	Director Representative of GIGABYTE Director Representative of Giga Investment Corp. Director Representative of Giga-Byte Communications Inc.	Director Representative of Giga-Trend International Investment Group Ltd. Director Representative of MyelinTek Inc.
Director	Tseng, Chun-Ming	Male	61 to 70	2022.03.08	3 years	Minghsin University of Science and Technology	Director Representative of GIGABYTE Director Representative of Giga-Byte Communications Inc. Chairman of Selita Precision Co., Ltd.	

2.1.3 Nomination and Selection of Board Members

According to the Company'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 the Articles of Incorporation, the Board is composed of the directors and requires the attendance of more than two-thirds of the directors. 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 Yeh, Pei-Chen, the Vice Chairman is Lee, E-Tay, and the General Manager is 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 are prohibited from representing other directors in the exercise of voting rights.

2.1.4 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 2023, 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.

2.1.5 Performance Evaluation

Since Giga Computing is currently a non-public company, no performance evaluation of the Board was conducted in 2023. In the future, as the internal governance structure becomes more complete, we also plan to introduce performance evaluations for the Board. This will help the Company assess the performance and effectiveness of board members, identify potential areas for improvement, and provide direction for development. Additionally, it will enhance the operational efficiency of the Board, improve the quality of its decision-making, and thereby promote the Company's competitiveness and sustainability.

2.1.6 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 in the most recent year. 4. Business execution expenses: The recent annual business-related 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. 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.

2.2 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 the "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 Office, General Administration Division
Short-, Mid-, and Long-term Goals	**Short-term goals (2024):** 1. The signing rate of the "Employee Code of Ethical Conduct" by new employees is 100%. 2. Plan for each employee to undergo at least one ethics-related education and training annually. 3. The investigation closure rate for cases of ethical corporate management violations is 80%, with a resolution time not exceeding 120 days from the receipt of the report. **Mid- and long-term goals (2025-2030):** 1. Maintain and implement ethics-related education and training for each employee, with at least one session per year. 2. The investigation closure rate for cases of ethical corporate management violations is 90%, with a resolution time not exceeding 90 days from the receipt of the report.
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, competitors, 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.
2023 Performance	1. The signing rate of the "Employee Code of Ethical Conduct" statement for new recruits was 100%. 2. The proportion of new employees receiving anti-corruption training is 51.74%. Moving forward, we will continue to strengthen this training and plan to implement anti-corruption and ethical corporate management training for all employees. 3. No reports were received during the year, and no employees violated the Ethical Corporate Management Best Practice Principles and Ethical Code of Conduct.
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.

2.2.1 Anti-Corruption Communication and Education

To implement ethical corporate management and promote 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 2023, 100% of new employees signed the "Employee Code of Ethical Conduct".

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 2023, 51.74% of new employees, totaling 74 individuals, completed anti-corruption education and 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 corporate social responsibility.

2.2.2 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 the "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, 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 2023, Giga Computing did not experience any violations of 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.

2.2.3 Whistleblower System

Giga Computing accept reports of suspicious behavior through various channels and has established a dedicated whistleblower mailbox. This mailbox is managed by a specialized internal auditor who reports directly to the Board, and it is available for use by both internal and external parties to actively prevent fraudulent activities. Upon receiving a report (including those not submitted via the whistleblower mailbox, such as reports from the General Manager and the Board, written letters, or the Human Resources Department), the Board will assign a dedicated unit to form a task force based on the nature of the report. This team will investigate the suspected fraudulent activities described in the report. The Company did not receive any whistleblower reports in 2023. In the future, the Company will establish relevant management measures in accordance with planning and legal regulations, and adjust the whistleblower operations in a timely manner.

2.2.4 Legal Compliance

Compliance with laws and regulations is the basic responsibility of enterprises and demonstrates a responsible attitude of enterprises. Giga Computing adheres to this principle by proactively understanding regulatory changes and making timely adjustments to ensure compliance. 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 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 regulatory 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. Ensure that the Company's various operating activities comply with laws and regulations.

In 2023, 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).

2.3 Risk Management

2.3.1 Risk Management Framework and Responsibilities

To enhance corporate governance and risk control capabilities, the Company employs a layered management approach and establishes internal regulations to conduct risk assessment 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 Department	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, 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

2.3.2 Key Risks and Response Strategies

The Company gathers industry risk trends and holds risk management meetings with various departments to identify potential risks in current operations from different perspectives. Risk factors are categorized and assessed alongside current response strategies and conditions to ensure all potential risks are within reasonable control limits, preventing serious financial, reputational, or operational impacts on the Company. In 2023, 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.

◆ 2023 Risk Items and Response Strategies

ESG Aspect	Governance	Governance	Governance	Governance	Environment	Social
Risk Item	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, etc.	The risk of sensitive customer and company data being extorted or leaked by external hackers.	Issues such as supply chain disruptions and material shortages caused by 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 disruptions or losses caused by GHG regulations, carbon taxes, carbon fees, as well as extreme weather events.	Talent retention, employee development, workplace environment, etc.

ESG Aspect	Governance	Governance	Governance	Governance	Environment	Social
Risk Item	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 Systems, 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 refers to the "RBA Code of Conduct". We have established 4 major 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.	Currently, the Giga Computing's Sustainability Promotion Team regularly conducts research and analysis on climate-related risks, in order 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. To ensure that employee safety, salaries, benefits, and workplace environment comply with relevant regulations and corporate policies, thereby reducing losses and risks caused by human resource factors. 2. The Company has 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):** The Company adopts an investment portfolio diversification strategy, making investments based on set limits to effectively control market risk. **Credit Risk:** The Company conducts management and credit risk analysis for each new customer before determining the payment and delivery terms according to the internal credit policy. By considering the customer's financial status, past experiences, and other factors, internal risk controls assess the creditworthiness of customers. **Liquidity Risk:** When holding excess cash beyond operational needs, the Company reallocates 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 a rigorous information security incident classification system and clearly defined the urgency of the incident. **Annual Information Security Internal Education and Training:** We have established an annual internal information security education and training system and conducted a phishing test on all employees to improve their ability to identify and respond to information security risks. **Management of Confidential Document Rights:** We have set up access levels for confidential company and customer documents to ensure that only personnel with appropriate authorization can access these documents.	**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 the 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:** To realize the vision of "Compute for the Future", Giga Computing has implemented internal incentives for obtaining patents and additional bonuses for energy-saving or green products, providing motivation for employees to continue its commitment to innovation.	**Introduce the TCFD framework:** In 2023, Giga Computing benchmarked international standards and introduced the TCFD framework for the first time. This included assessing and identifying climate risks and opportunities, as well as establishing a climate governance framework and processes. **Self-conducted GHG inventory:** Giga Computing has consistently followed its parent company GIGABYTE, in conducting ISO 14064-1 GHG Inventory Standard. In 2023, for the first time, it conducted an independent GHG inventory using Giga Computing as the boundary, focusing on its own operational scope. In the future, based on the inventory results, subsequent reduction plans will be made to implement the Company's carbon management.	**Talent Cultivation:** We are committed to cultivating 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:** Every year, we reserve a budget for employee training to improve employees' professional skills and leadership capabilities. At the same time, we encourage our employees to improve themselves and participate in external training courses. **Subsidy Policy:** In order to encourage employees to improve their professional capabilities and increase industry competitiveness, we have established a certification allowance and reward system to recognize and reward their efforts.

2.4 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 Company's 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 Office
Short-, Mid-, and Long-term Goals	**Short-term goals (2024):** 1. Zero major information security incidents. 2. Conduct regular audits for the ISO/IEC 27001 information security certification annually. 3. Each employee must undergo at least 1 information security education and training annually, along with occasional social engineering drills. Those who do not pass these drills will be required to undergo additional training. 4. Expand the depth of evaluation, continue to enhance the maturity of information security and the improvement of the information security management system. 5. Strengthen supply chain information security joint defense. 6. Conduct information security policies advocacy and training. 7. Ensure that the enterprise's information security and privacy protection measures comply with local and international regulatory requirements. **Mid- and long-term goals (2025-2030):** 1. The ISO/IEC 27001 information security certification is maintained through regular audits, with continuous monitoring of regulatory updates. 2. Each employee must undergo at least 1 information security education and training annually, along with occasional social engineering drills. Those who do not pass these drills will be required to undergo additional training. 3. A comprehensive information security system will be constructed by referencing more extensive information security frameworks. 4. Deepen the cultivation of corporate safety culture and raise the safety awareness of employees and suppliers. 5. Adopt more advanced technology and protective measures. 6. Ensure corporate compliance and regulatory compliance. 7. Establish an emergency response and crisis management mechanism with suppliers.
Action Plan	1. Continue information security education and training and implement social engineering drills to strengthen employees' information security awareness and vigilance, and to refine the information security framework for compliance and customer needs. 2. Vulnerability scanning and penetration testing are performed occasionally to prevent and prepare for crises. 3. In compliance with international information security standards (NIST CSF framework) and domestic and foreign information security regulations to implement information security and privacy protection with a more rigorous management spirit. 4. The Information Security Promotion Committee holds a management review meeting annually to review and discuss matters related to the information security management system.
2023 Performance	1. No major information security incidents occurred. 2. Implementing high-sensitivity data encryption measures. 3. Obtained ISO/IEC 27001: 2022 and CNS 27001: 2023 Information Security Management Systems 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. 6. Conducted two social engineering drills and provided enhanced training courses for employees who do not pass. 7. Implementation of information security policies advocacy and training.
Grievance Mechanism	Giga Computing's Privacy Policy

2.4.1 Information Security Policy

The General Manager Office is responsible for formulating information security policies, risk assessment, and implementation and follow-up of countermeasures. The CIO occasionally reports to the General Manager each year. In order to reduce the risk of non-compliance and increase customer trust, Giga Computing introduced the ISO 27001 Information Security Management Systems in 2023 to establish a complete and systematic approach to manage and protect 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. Regular information security attack and defense drills are held to strengthen the information security awareness of internal employees.

2.4.2 Responsible Unit for Information Security

To effectively promote and manage all aspects of information security 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.

2.4.3 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.

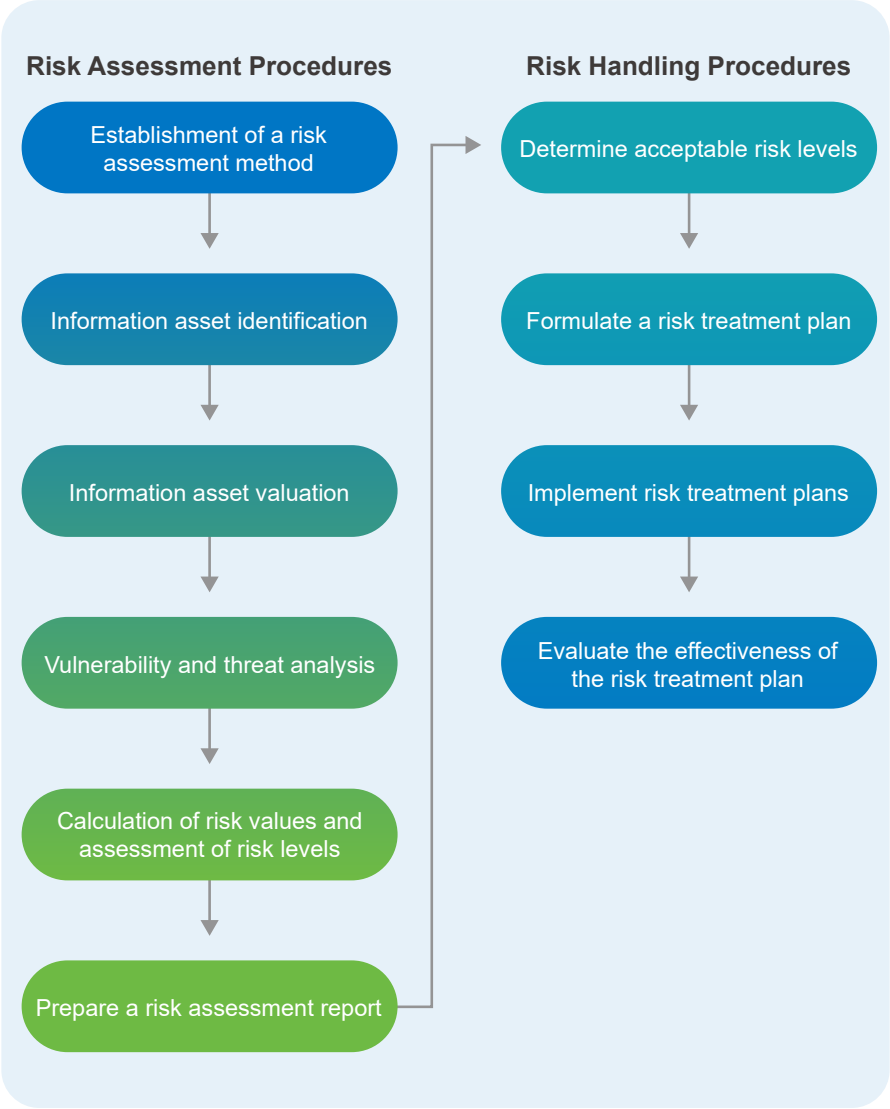
Information Security Implementation Team

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. Compile 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.

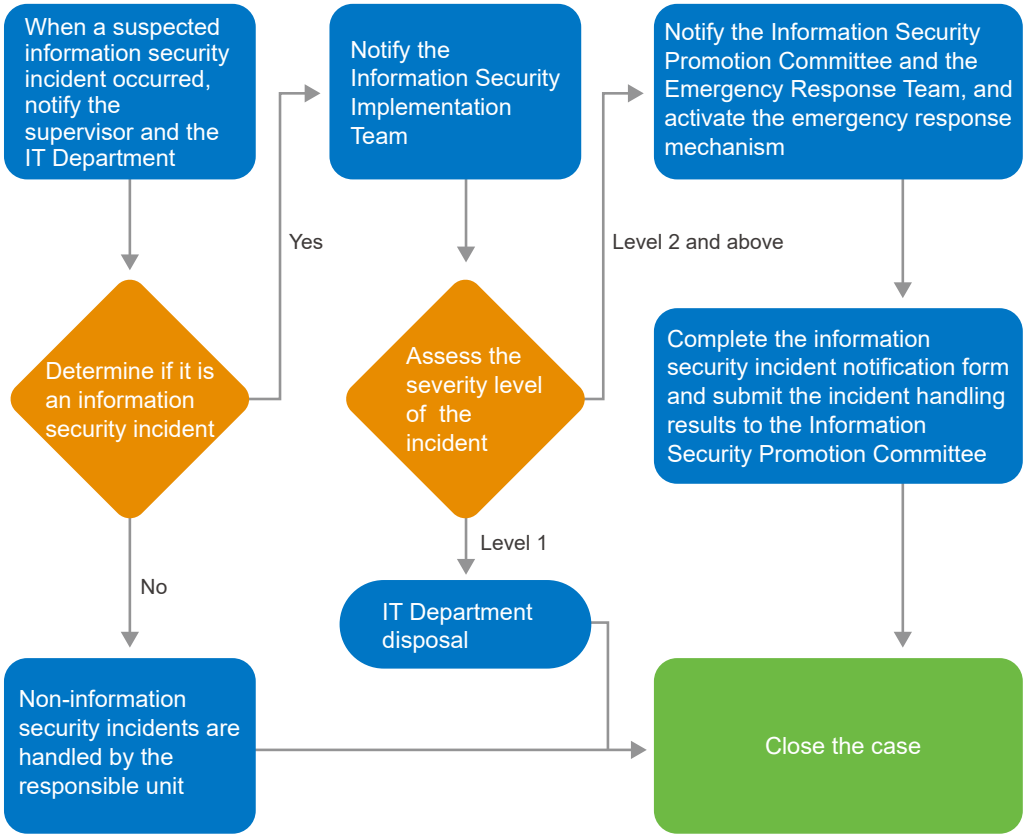
Risk management refers to the risk control process for information assets that include the "Risk Assessment Procedures" and "Risk Handling Procedures". The main operating items are shown in the figure below:



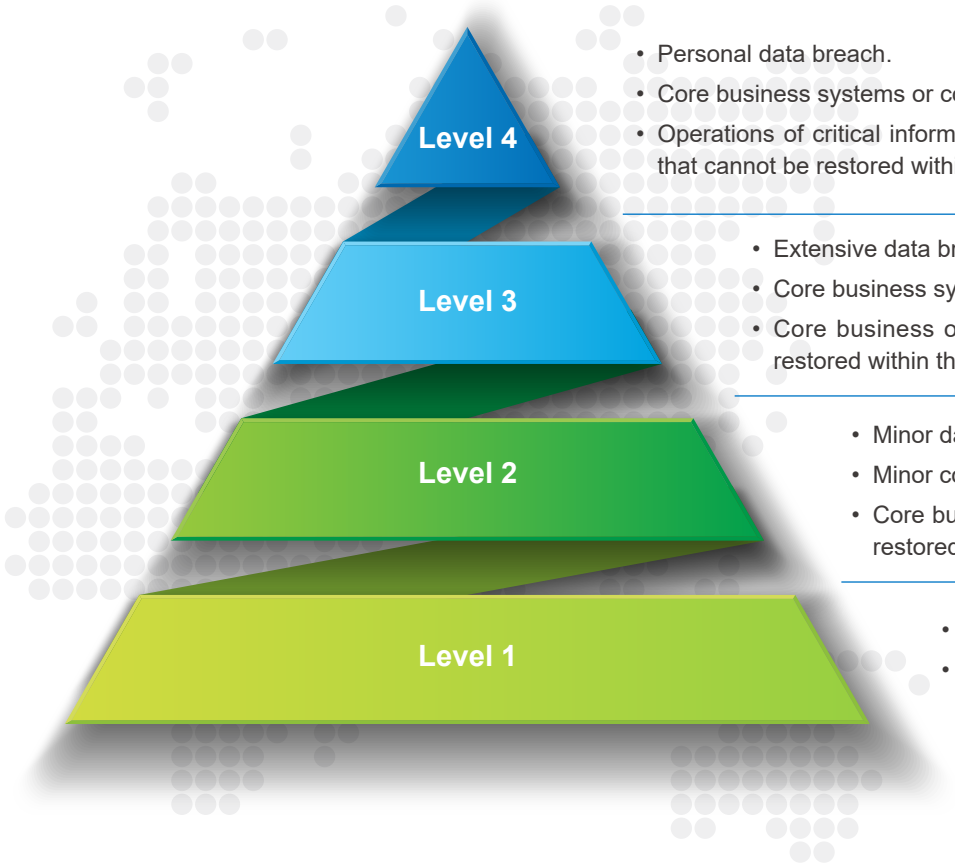
2.4.4 Procedures for Reporting Information Security Incidents

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 or not 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 team will be notified to assess whether or not to activate the Emergency Response Team operations.

In the event of an information security incident, the IT 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



- 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.

- 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.

- 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 was restored within the acceptable downtime threshold.

- 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.

2.4.5 Countermeasures for Information Security

Information security training is conducted based on the business content and role requirements of each position. Information security personnel from the IT Department must receive at least 2 hours of information security training annually. New employees should 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 should use the internal website or email to inform internal employees of the latest information security threats and preventive measures.

Course Title	Course Topic	Form of Implementation	Participants	Number of Trainees	Course Hours	Total Training Hours
ISO 27001: 2022 Information Security Management Systems Lead Auditor Training Course	Cybersecurity professional certification recognized by the Administration of Cyber Security, Ministry of Digital Affairs	Physical	Information Security Personnel in the IT Division	1	40 hours	40 hours
Information Security Training	Information, email security and cybersecurity awareness	Physical	Information Security Personnel in the IT Division	4	2 hours	8 hours
Information Security Awareness Training	Promote the Company's information security policies and enhance security awareness	Physical	New employees	143	10 minutes	23 hours and 50 minutes
Intensive Social Engineering Training	Enhance security awareness and vigilance	Online	Employees who did not pass the drill	77	30 minutes	38 hours and 30 minutes
Total				225	-	110 hours and 20 minutes

Employees must comply with the relevant safety regulations when entering and leaving the office and server room. Employees shall comply with relevant laws and regulations when performing their duties. If there is any violation (such as computer leakage, personal data theft, etc.), they will be dealt with according to the Company's work rules depending on the severity.

In the event of an information security incident, the IT Division should document the incident, including the facts of the incident, the potential impact, loss assessment, requests for support and the measures taken in response.

1. When the incident has a low impact and minor consequences, involving only internal units and causing slight damage (such as internal security issues, computer virus infections), and the affected unit 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 affected unit 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 convener of the Information Security Promotion Committee, who will decide whether or not to activate the emergency response mechanism.
3. In the event of a security incident, the leader of the Emergency Response Team should be responsible for contacting the team, coordinating and supervising the execution of tasks by key business process owners, and managing the allocation of resources.
4. If the security incident level is "Level 2" or above, the affected unit 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 coordinating company resources and providing necessary assistance as needed. When an information security incident requires external communication, the leader of the Emergency Response Team must report to the CIO and assist the spokesperson of Giga Computing in communicating the situation and the response measures to the public. In 2023, Giga Computing did not experience any major information security incidents classified as "Level 4" or above.