Basic approach

We consider the improvement of corporate governance to be a key business issue for ensuring that we have the appropriate business execution structure, and for raising our performance, value, and social credibility.

Corporate governance structure

We have an executive officer system in place, in which our executive officers implement key business execution under the supervision and monitoring of our Board of Directors and Board of Auditors.

Board of Directors

Currently comprised of eight directors, the Board of Directors determines and manages the implementation of the basic points of business execution for our corporate management, based on our articles of incorporation, the rules of our Board of Directors, and other relevant rules and regulations.

In principle, the Board of Directors meets monthly to facilitate swift decision-making and facilitate intimate and lively discussions between directors. We also have a system which avoids making biased decisions by having multiple representative directors and clarifying each director's area of responsibility.

Board of Auditors

We have a Board of Auditors composed of three company auditors including two external auditors. The company auditors attend important meetings such as board meetings and audit the execution of duties by the directors by inquiring about the status of their business operations.

Executive officers

Our executive officers make business operations efficient by leading organizations that oversee important functions and executing business operations based on Board of Director decisions on fundamental matters and the discretion allocated by relevant regulations. Opportunities are also provided for executive officers to regularly provide business reports on their areas of responsibility to the directors overseeing them. This is designed to make our auditing system function timely and appropriately.

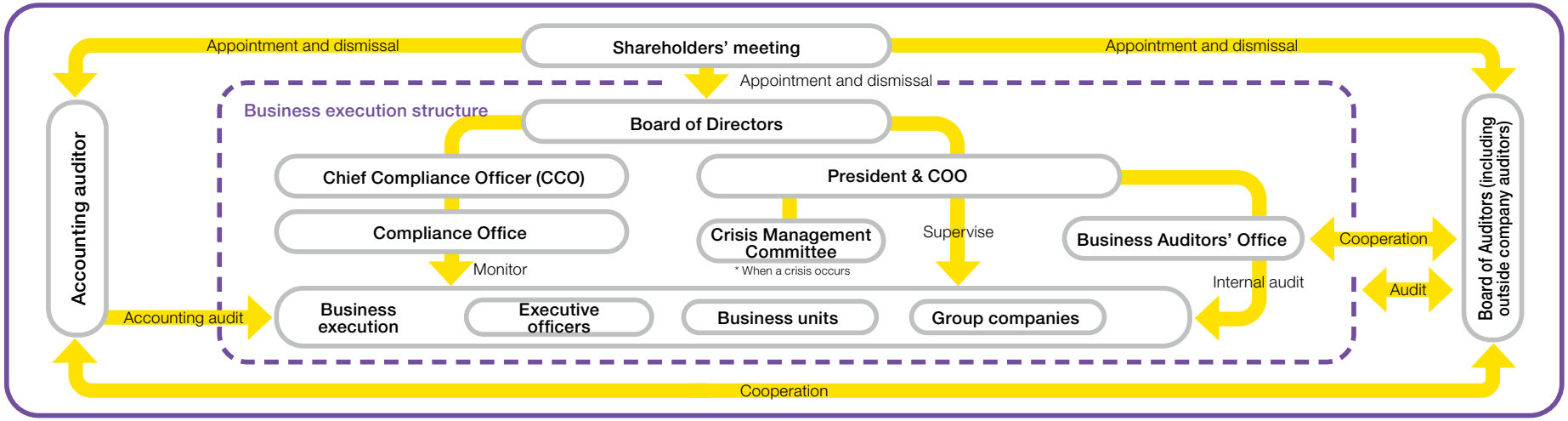
Internal control system

We are implementing various measures to ensure that we comply with applicable laws as well as the company's articles of incorporation in our business execution.

Based on a business division system, our businesses are arranged to facilitate flexible operations according to the characteristics of each business. At the same time, to exercise consistent control over the Group with our Head Office sections playing a central role, we also stipulate core organizational rules and regulations on delegation of authority while clarifying each organization and its allocated duties and authority, based on which we build our operational structures. Opportunities for decision-making and reporting at each level are also provided in order to ensure the business execution and reporting in each department and ensure that top management is making decisions, inspecting, and communicating with each department.

For Group companies we have established our Governance Rules for Associated Companies. We also clarify rules for business operations and conduct both operational and accounting audits as needed.

Corporate governance structure (organizational structure)



Basic approach

In order for INOAC to satisfy its corporate social responsibilities and expectations from customers, it is not enough to simply observe the applicable laws. Employees must also recognize their social responsibilities as part of the corporation. We strive to implement thorough compliance that goes beyond simply defining a company policy and observing the applicable laws by also holding each individual employee to high ethical standards in their actions.

Implementation system

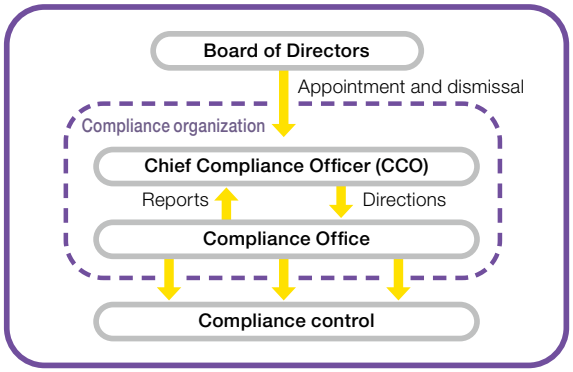
With authority independent of our directors and executive officers, our Chief Compliance Officer (CCO) runs the Compliance Office, taking measures and actions for compliance-related matters. Working together with the Compliance Office, with the CCO playing a leading role, we conduct compliance activities while finding ways to strengthen our overall global coordination.

If any compliance violations arise, the CCO directs the Compliance Office as the person in charge of the response. The CCO establishes a task force at Head Office to address the violation in a centralized manner according to the level of impact.

We continuously improve the program that determines our compliance organization through revisions made regularly by the CCO. The Compliance Office also hosts a Global Compliance Evaluation Conference once per year.

Through periodical risk assessments by the Compliance Office, the CCO identifies areas where particular efforts are warranted, and nominates compliance officers to manage each area according to the basic compliance policy. These compliance officers work together with the Compliance Office and hold breakout sessions on a quarterly basis. In addition to compliance-related matters, various challenges and risks that could arise in each area are discussed in breakout sessions to facilitate sound corporate management and thorough risk management for the organization as a whole. As a policy for addressing important matters each area, we formulated our Compliance Policy which we are now rolling out worldwide. We are implementing consistent governance internationally in addition to domestically by making observance of this policy mandatory for all INOAC Group companies.

Organizational chart



Compliance training

We believe that systematic and continuous compliance training is necessary for all members of our organizations to understand what to observe, what to avoid, and incorporate that understanding into their actual work.

As an initiative of the *Mamoru project*, we are organizing training points aligned with each key area, and dividing them into those which all officers and employees should undergo, those to undergo at career stages, and those to undergo by job type. Based on this, we are conducting mandatory companywide training and regular training at major intervals in employees' careers (compliance training in training for new employees, employees hired mid-career, overseas assignment candidates, those handling core functions, etc.). In addition, we conduct separate compliance trainings according to the characteristics of each region and department.

In mandatory companywide training, training on the action guidelines comes first. Corrupt practices and relations with antisocial forces are examples of behavior patterns to be eliminated through this training. We also offer and implement training frameworks for other important laws, regulations, and high-risk areas.

* "Mamoru" is a Japanese word that means "to protect" or (in the context of laws) "to comply with."

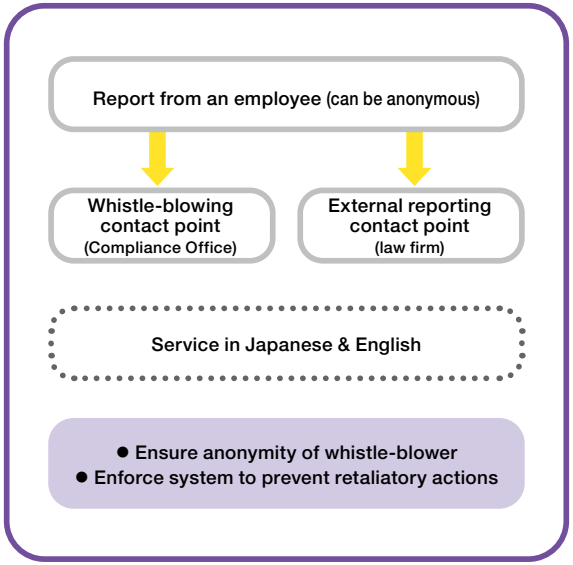
Whistle-blowing system

We have established a whistle-blowing system to enable everyone who works for or with the INOAC Group to consult or report matters involving compliance violations that have or might have occurred.

Our whistle-blowing system connects both internally (to the Compliance Office) and externally (to a law firm). The system offers service in English in addition to Japanese.

Based on the relevant regulations, we enforce a system that ensures confidentiality of the whistle-blower's identity and prevents the occurrence of retaliatory actions targeting those who report through the system.

Whistle-blowing system overview



Implementing the Mamoru project

In order to operate soundly as a corporation and thoroughly ensure compliance, we believe that we must create an open corporate culture in which all members of our Group feel free to speak up. For that reason, we are creating a more familiar and positive impression by engaging in efforts with *Mamoru* as the keyword, intentionally expressed in roman letters even in Japanese, as opposed to "compliance" and "integrity" which are expressed in katakana characters. We are rolling out *Mamoru* globally as-is in a unified manner while defining the following three phrases as its underlying spirit.

(1) Comply with the Rules
(2) Safeguard Your Colleagues
(3) Protect Yourself

Mamoru, meaning to "protect," encourages individual employees to not only use the aforementioned whistle-blowing system, but also to consult with the Compliance Office or those around them whenever feeling even somewhat suspicious of something in their work, thus also *protecting* themselves and their colleagues. As part of this project, we are fine-tuning and regularly revising our compliance training as outlined below in order to more specifically communicate to all employees and those identified according to their job details about what should be "protected" as stipulated for *Mamoru*.

The word *Mamoru* is a message being communicated directly from top management to INOAC locations throughout the world along with our compliance policy and the contact points, and is published on the intranet within the INOAC Group to always be accessible to all officers and employees.

We are building a foundation that can bolster the value of our company in an even more transparent manner by opening up the lines of communication between members of the INOAC Group.

Continuous awareness-raising activities

With *Mamoru* as the keyword, we continuously have our compliance officers directly communicate to all employees about what should be "protected" in the areas each officer is responsible for.

In our regularly published in-house magazine, we currently have a regular section called *Mamoru* in which a different officer shares information each time. This section has been published on an ongoing basis since 2024, including appearances by the CCO and officers from human resources, quality, procurement, and more.

まもる
mamoru

Governance | Information security

Basic approach

Based on our awareness that the information assets that we handle are key business resources and assets, we offer products and services that are steady and stable. To also ensure the confidentiality, integrity, and availability of our information assets, we identify information security risks on an ongoing and organizational basis, and take the appropriate measures to manage them. Furthermore, as we operate business throughout the world, we are formulating a comprehensive information security policy that takes the legal and cultural environments of each country and region into consideration.

Implementation system

Our Information Security Committee was established in September 2022. The aim of our activities is to implement these globally throughout our organizations as we also work to reduce occurrences of cyber incidents and put response measures in place.

Roles

Chief Information Security Officer (CISO):
Has decision-making authority and full responsibility for information security measures.

Director of the Information Security Committee's administrative office:
Responsible for the operation of the Information Security Committee.

Information Security Committee's administrative office:
Reviews and implements information security measures.

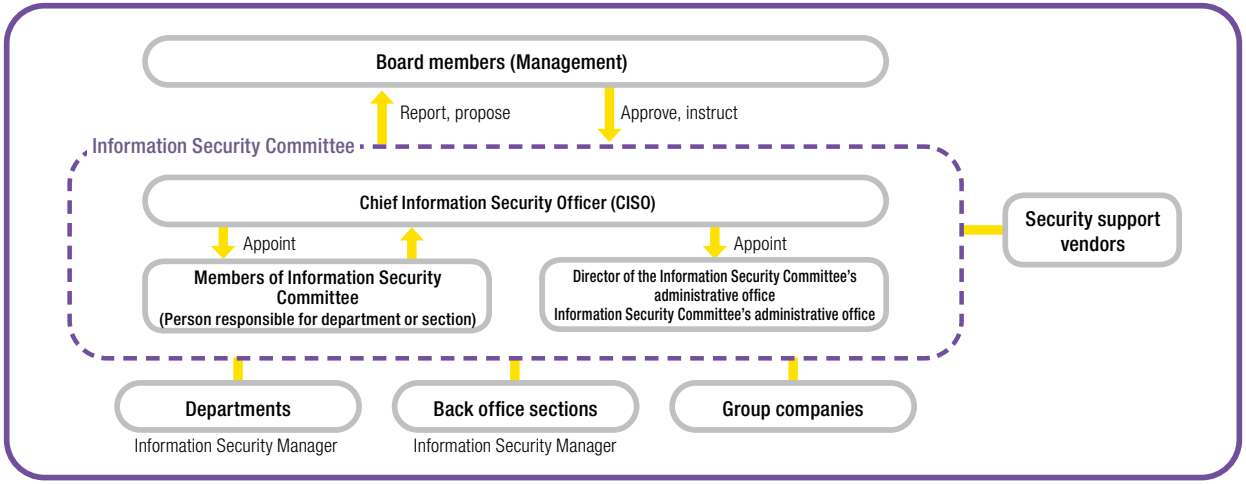
Members of Information Security Committee:
Responsible for implementation of information security measures in each section.

Information Security Manager:
Implements information security measures in each section.

Activities

- Conduct in-house training for preventing security incidents at least 2 times/year & new employee training
- Create internal regulations & guidelines
- Establish the flow of reviews when implementing systems
- Establish & implement management rules according to the confidentiality of information
- Create and conduct training on flows for incident handling to enable swift responses when security incidents occur
- Create business continuity plans for when security incidents occur
- Implement security incident defense measures using log correlation analysis & vulnerability assessment tools
- Create a communication network for emergencies
- Comprehend the status of information security implementation in the supply chain
- Facilitate activities to bolster information security at overseas group companies

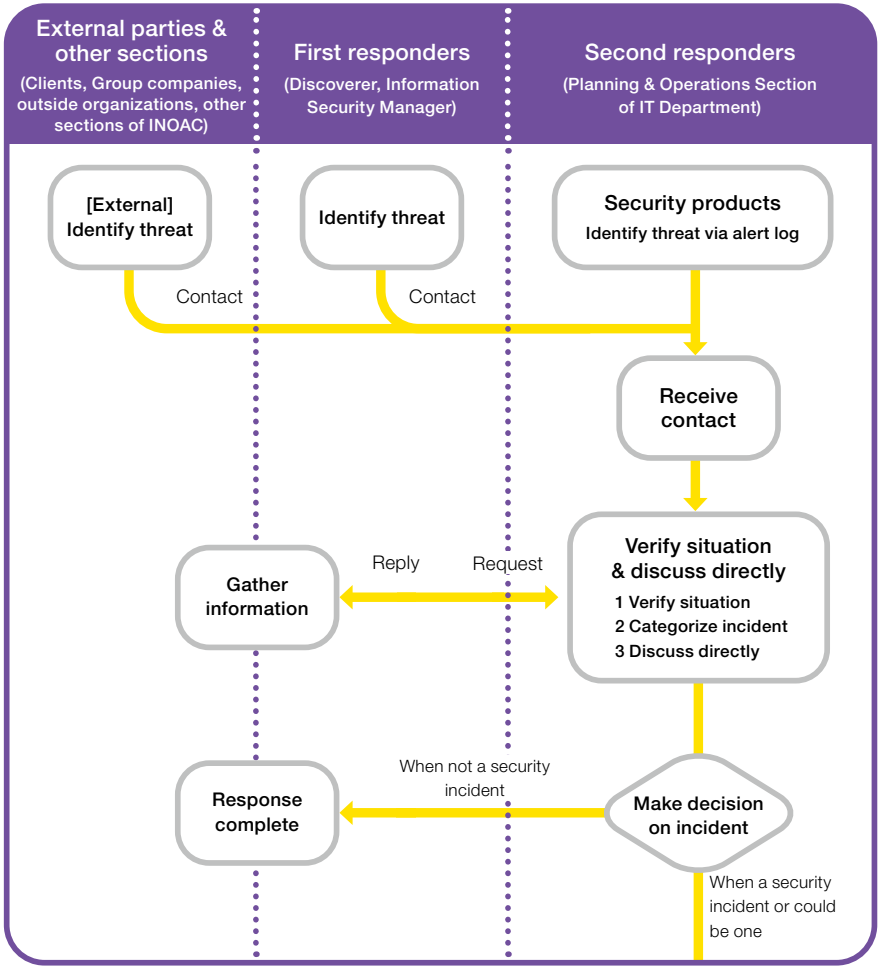
Organizational chart (in normal circumstances)



Handling incidents

We have defined Accident Level 3 as “severe incidents that impact clients and other external stakeholders,” and we handle them according to our information security management structure for emergencies, as stipulated by our Information Security Committee.

Flow of incident handling (excerpt)



Goals & results of activities

Goals	2024 results
Achieve 100% of Level 1 & Level 2 items in Cybersecurity Guidelines V2.2 by March 2026	Achieved 97% of Level 1 & Level 2
Understand the state of measures to strengthen information security by suppliers who handle important information, and facilitate such measures	Conducted surveys on the state of measures to address information security at particularly important suppliers
Conduct training for all employees including manufacturing site personnel	Conducted information management training for all employees
Implement cloud services evaluation standards	Evaluated major cloud services related to our business activities

Protecting personal information

We consider protecting the personal information that we acquire and manage through our business activities to be an issue of the utmost importance. We fulfill our responsibility as a trusted company by valuing the privacy of our customers and employees and thoroughly ensuring secure and appropriate management of their information.

For the handling of personal information, we adhere to the following principles in line with our Personal Information Protection Regulations.

Principles on handling personal information

Adhere to laws, regulations & rules	For more details, please see “Protection of Personal Information” on our website. (https://www.inoac.co.jp/en/privacypolicy/)
Clarify purpose of use	
Manage and protect properly	
Restrict provision to third parties	
Train employees & raise awareness	Conducted information management training for all employees