Risk Management

Basic Philosophy

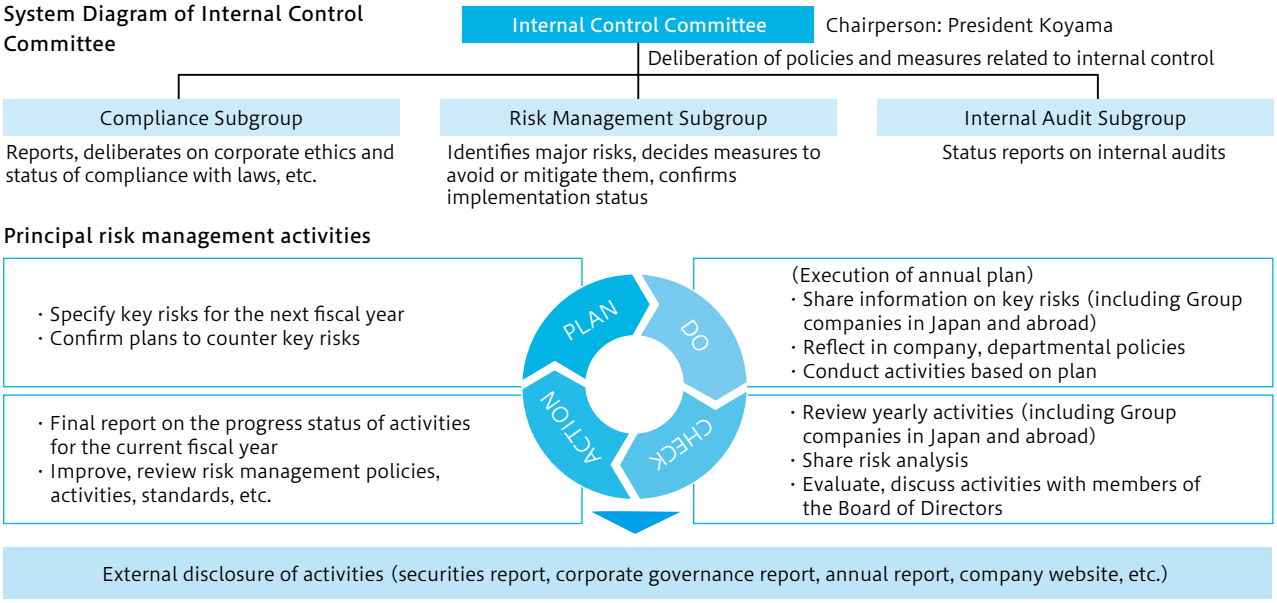
We are working to prevent risks that could have grave consequences for management and to minimize damage in adverse events. For these purposes, we identify risks in each function and make decisions on how to respond in Board of Directors, Internal Control Committee and general meetings throughout the company.

An Internal Control Committee headed by the company president identifies key risks, determines measures to counter them, and checks on the progress in executing these measures. In this way, these measures are made more effective.

In addition, initiatives to deal with key risks or unexpected business risks due to political instability or other external factors are discussed regularly by the Board of Directors, and continuous improvements are made.

Moreover, Risk Management and Response Guidelines have been established. These guidelines show the behaviors to adopt to prevent potential risks and to respond to problems appropriately and quickly. Parts of the BCP plan are discussed by the Board of Directors with respect to COVID-19. With consideration of the status of infection spread, actions taken to minimize the impact of COVID-19 include (1) preventing infection by promoting work from home, regulating business trips and visitors, and cancelling company internal events, (2) implementing measures for the event that an infection occurrs in an employee, (3) maintaining our production network by monitoring issues, including at our suppliers, and (4) introducing profit improvement measures.

System Diagram of Internal Control Committee



Principal risk management activities

External disclosure of activities (securities report, corporate governance report, annual report, company website, etc.)

Response to Key Risks

Operating foundation risks and business strategy risks based on the business environment are assessed from the perspective of impact on operations (financial impact, etc.) and possibility of occurrence (frequency), and key risks are identified.

Key risks are reflected in company policy as important action items, and initiatives are made to mitigate or prevent risks.

Examples of Key Risks

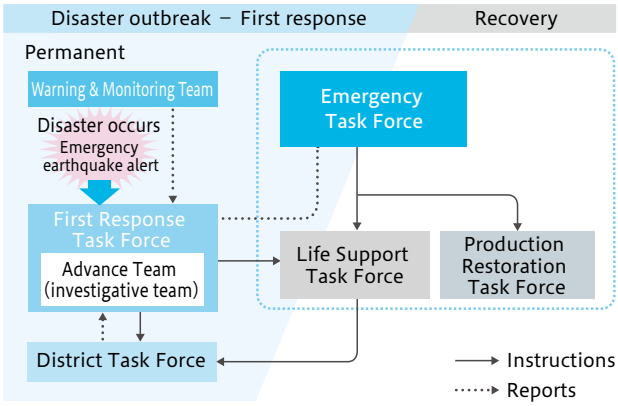
Classification		Main key risks
Size of risk Impact on operations (financial impact, etc.) × Possibility of occurrence (frequency)	Large	•Large-scale disaster (earthquakes, storm and flood damage, etc.) •COVID-19 (infection prevention, production system maintenance •Risk/opportunity and handling based on TCFD •Carbon neutrality handling •DX handling •Impact of Russia/Ukraine situation •Cyberattacks/scam email •Recall due to serious quality problem •Human injury, operation shutdown due to serious labor accident
	Medium	•Leakage of confidential information •Traffic accidents (causing serious damage/injury) •Occurrence of harassment
	Small	•Anti-trust law violations •Business operations of partner companies •Interruption of business activities due to fire or explosion accidents

Crisis Management Project in Anticipation of Large-Scale Earthquake Disasters

A crisis management system has been put in place for the event of a massive disaster, such as the predicted Nankai Trough earthquake or natural disasters due to climate change. This system is based on the principles of human life first, community support, and early recovery. Specifically, in addition to infrastructure and system measures based on a crisis management project, resilience training has been conducted more than 160 times for directors and members of antidisaster departments since FY2013. These efforts are based on the company's belief that improving the skills of response personnel is essential. Specific procedures for the recovery of affected buildings, facilities, and processes have also been established, and for alternative production in a production recovery system.

Recovery training for design drawings and other data is also carried out so that product development can be continued even after disasters. In addition, workshops to strengthen crisis management not only in Toyoda Gosei companies but also at Group companies and suppliers are conducted regularly. Assessments using anti-earthquake measure implementation status check sheets, clarification of weak points with graphs, introduction of responses taken at Toyoda Gosei and other companies, and cooperative preparation of business continuation plans (BCP) are carried out.

Disaster Response



Initiatives to Date

Classification	Measures
Facility and equipment measures	• Earthquake resistance measures for buildings and facilities • Establishment of a disaster prevention center to serve as an operations base for the entire company for anti-disaster department operations • Equipping all locations with a multi-channel access radio system (which is used in Japan for various purposes, from daily work to emergency and disaster situations) and satellite phones • Installment of a crisis management server (earthquake-resistant structure) and emergency power generators • Operation of a disaster recovery system for restoration of damaged systems and data centers (special facilities equipped with and operating computers, data communications, and other devices)
System measures	• Introduction of site and building safety decisions • Earthquake bulletin and employee safety information system training • Maintenance of supply chain information • Preparation of a business continuity plan (BCP)
Skills	• Continuation of resilience training (disaster simulations)

Strengthening of Global Risk Response

The status of risks, not just domestic but also frequently occurring global risks (tightening supply of parts and raw materials, COVID-19-related operation shutdowns, Ukraine situation and more), is identified, the early situation both in Japan and internationally is grasped (issuance of a weekly BCP), and necessary actions are taken globally. Standardization is also underway so that measurements can be taken by domestic and international locations on their own initiative, strengthening the response to key risks seen in the business environment of each company.

Basic Policy for Cybersecurity Measures

To strengthen the control of confidential information, annual checks of the compliance status of each division based on company confidentiality management regulations are conducted together with onsite audits. Self-inspections are also done at Group companies in Japan and overseas, as well as at major suppliers.

Confidentiality officers are assigned in all departments, and confidentiality education activities are conducted based on information system security operating standards and a confidential information management manual. At domestic and international Group companies and major suppliers, specific measures are stratified and executed based on the size of the impact on Toyoda Gosei and inspection results for cyber risk measures at each company. Regular reports and discussions are conducted in all company boards, and cybersecurity measures are taken together globally.

Main Cybersecurity Measures

Classification		Measures (domestic and international Group companies and suppliers respond in accordance with the size of the impact)
Prevent leakage due to negligence	Facility and equipment measures	• Printing restrictions with ID card authentication for multifunction printers and dedicated drawing printers
	System measures	• Data encryption on all personal computers • Security measures when sending emails out of the company (mandatory cc to superior's email address, encryption of attached files)
Prevent leakage due to malice	Facility and equipment measures	• Increased surveillance cameras • Restrictions on writing onto external storage media • Installation of wire locks to prevent PC theft
	System measures	• Confidentiality pledge • Monitoring of system use records, access log records • Stricter applications for taking items from premises • Strengthened hacking prevention measures (Internet) • Restricted access to file servers • Prevention of unauthorized connection to terminals brought in from the outside
Educational activities (morale measures)		• New employee education • On-site inspections of each department • Company-wide voluntary security control inspections using check sheets • Training in responding to targeted email attacks