Risk Management

Fundamental Approach Toyota has been working to reinforce its risk management structure since the recall issues in 2010. In June 2010, Toyota established the Risk Management Committee (now Sustainability Meeting and ESG Committee) and appointed risk managers globally and at each section to comprehensively prevent and mitigate the impact of risks that could arise in business activities.

Organization and Structure

Toyota has appointed a Global Chief Risk Officer (CRO) as a head of global risk management, who oversees significant risks and takes leadership to respond to significant global emergencies. Beneath the Global CRO are Regional CROs appointed to manage its own risk management structure.

Within the head office (such as Accounting and Purchasing), risk management is assigned to chief officers and their sections, while in each in-house company, risk management is assigned to the company president and their company. They coordinate and cooperate with the regional head offices and with each section.

To oversee and mitigate global risks, risks in business are identified and significant emerging risks are reported and reviewed by the ESG Committee.

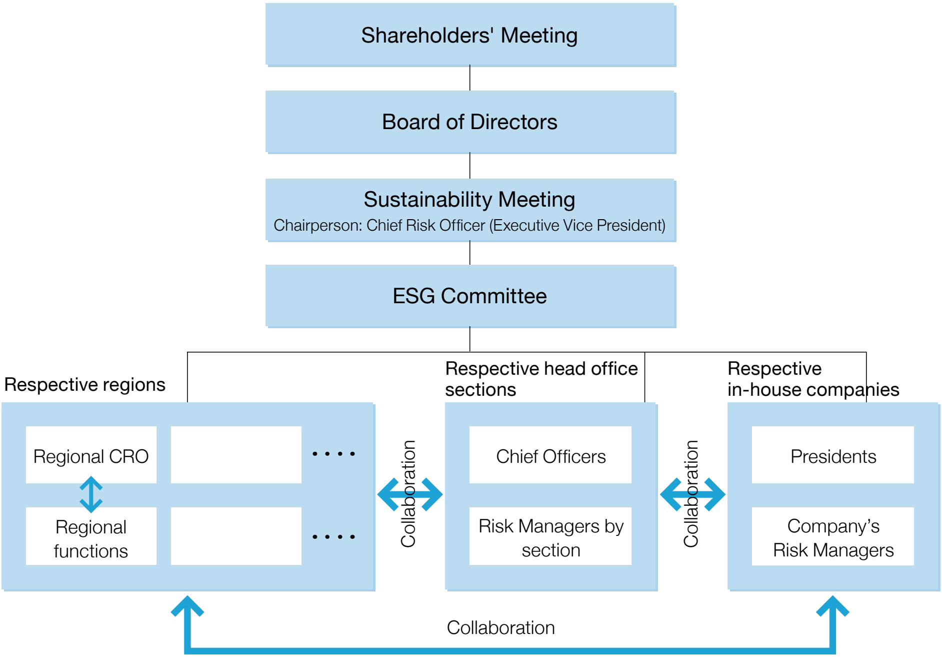
In addition, as a business supervisory body, results from the ESG Committee are reported in Sustainability Meetings.

To respond to emerging risks in recent years, Toyota advances measures related to information security and business continuity management (BCM).

Risks related to Toyota's businesses that could significantly impact the decisions of investors are listed in *Form 20-F*: Industry and Business Risks; Financial Market and Economic Risks; Regulatory, Legal, Political and Other Risks.

Form 20-F Web https://www.toyota-global.com/investors/ir_library/sec/

Organization



Initiatives for Information Security

With cyber attacks becoming more sophisticated and complicated, the targets of cyber attack are not limited to confidential information and information systems, but also include the networks of systems that control plant facilities and vehicles (such as on-board device systems). The importance of information security is increasing for Toyota.

Toyota will ensure the safety and security of our customers from cyber attack threats. Toyota considers it our social responsibility to protect our customers' personal information and therefore is reinforcing information security by governance and risk management.

In June 2016, TMC and its consolidated subsidiaries together established Information Security Policy to clarify the information security basic policy and initiatives.

Information Security Policy (Toyota's Basic Approach)

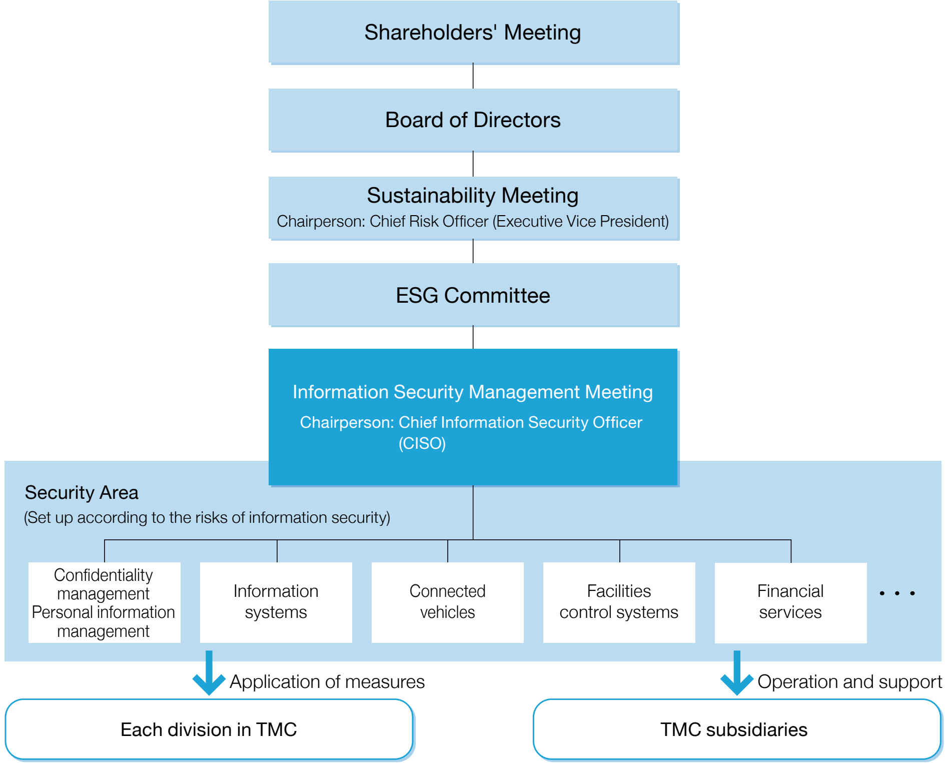
1. Compliance
2. Maintenance of stable business infrastructure
3. Providing safe products and services
4. Contribution to the establishment of safe cyberspace
5. Information security management

Information Security Policy Web https://www.toyota-global.com/sustainability/governance/risk-management/pdf/information-security-policy_en.pdf

Organization and Structure

Under the Chief Information Security Officer, security officers are respectively assigned in the individual security fields to promote activities.

Details of activities in each security field and overall common issues are shared and discussed at Information Security Management Meetings to improve information security throughout Toyota.


Shareholders' Meeting
Board of Directors
Sustainability Meeting
Chairperson: Chief Risk Officer (Executive Vice President)
ESG Committee
Information Security Management Meeting
Chairperson: Chief Information Security Officer (CISO)
Security Area
(Set up according to the risks of information security)
Confidentiality management Personal information management
Information systems
Connected vehicles
Facilities control systems
Financial services
• • •
Application of measures
Operation and support
Each division in TMC
TMC subsidiaries

Initiatives for Information Management

Toyota has established the All Toyota Security Guidelines (ATSG) covering TMC, its subsidiaries and affiliates seeking to comprehensively prevent information leaks and emerging risks of cyber attacks.

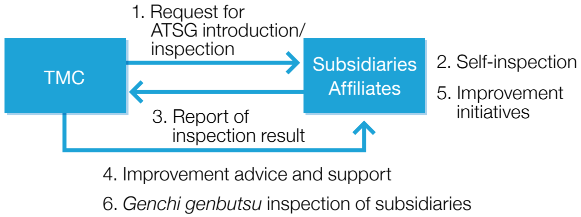
ATSG ensures information security through a multi-faced approach: through organization, human resources, technical security, physical security, and incident/accident response. To cope with recent environmental changes and sophisticated cyber attacks, ATSG is revised periodically (latest update in April 2018).

By annually inspecting the information security initiatives being taken at each company in line with the ATSG, Toyota is working to ensure continuous maintenance and improvement. Furthermore, in FY2019, TMC will begin checking its subsidiaries (*genchi genbutsu*) for further improvements.

All Toyota Security Guidelines (ATSG)

1. Organizational management measures (establishment of organization and rules)
2. Human resources management measures (employee training, etc.)
3. Technical management measures (network security, etc.)
4. Physical management measures (entry and exit controls, etc.)
5. Establishment of incident/accident response

Structure for ATSG Implementation at Subsidiaries and Affiliates


1. Request for ATSG introduction/ inspection
TMC
Subsidiaries Affiliates
2. Self-inspection
5. Improvement initiatives
3. Report of inspection result
4. Improvement advice and support
6. *Genchi genbutsu* inspection of subsidiaries

For personal information, individual education ensures that employees are well aware of the importance of following the law and handling information appropriately. We have responded to the Amended Act on the Protection of Personal Information (Japan) and the GDPR[1] (Europe), and will continue to endeavor to protect personal information.

As for automobile-related matters, in Japan and the United States, Toyota has joined the Auto-ISAC[2], an industry-wide community for auto makers to share information on cyber attack case examples. Toyota is making efforts to improve cyber security by monitoring the latest trends.

[1] GDPR: General Data Protection Regulation

[2] Auto-ISAC: Automotive Information Sharing & Analysis Center

Business Continuity Management at Toyota

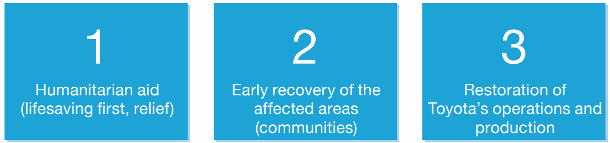
Although Toyota was not directly affected by large-scale disasters such as the Great East Japan Earthquake and the Thailand floods, our production operations stopped for a long period of time which caused inconvenience to customers both in sales and services.

There are deep concerns about the Nankai Trough Massive Earthquake occurring, as the Toyota Group Companies' main functions are concentrated in the area. It is predicted that a large scale earthquake would severely impact our production and logistics operations.

To be prepared for such disasters, the Business Continuity Plan (BCP) was established to facilitate early recovery of business operations with limited resources.

In order to contribute to enriching lives of communities, Toyota will work on disaster recovery according to the Basic Guidelines. This guideline was followed in the Kumamoto Earthquake (April 2016).

Toyota's Basic Guidelines (Priorities during a Disaster)


1
Humanitarian aid (lifesaving first, relief)
2
Early recovery of the affected areas (communities)
3
Restoration of Toyota's operations and production

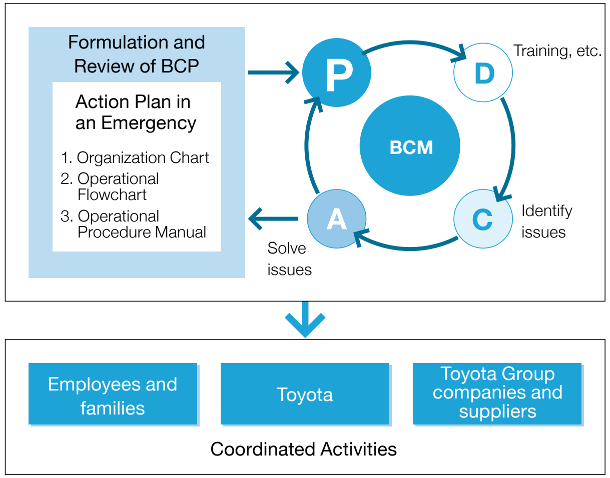
Business Continuity Management at Toyota

The PDCA[3] is implemented and continuous improvement is undertaken through training, etc., to constantly raise the practical effectiveness of Toyota's BCP.

These activities are identified as the Business Continuity Management (BCM), which are delivered through coordination among employees and their families, Toyota Group companies and suppliers, and Toyota.

Through this process of formulation and review of the BCP, we aim to develop risk-resilient organization, workplaces, and individuals.

[3] PDCA: The circular process of Plan-Do-Check-Action for continuous improvement



Humanitarian Aid and Early Recovery of Disaster-affected Areas (Communities)

Toyota has concluded comprehensive disaster support agreements with local governments (Toyota City, Miyoshi City, Tahara City, and Susono City). In accordance with the Basic Guidelines, these efforts will give priority to disaster recovery and contribute to building disaster-resilient communities. Humanitarian support and regional recovery assistance are to be provided under mutual cooperation with local governments. Toyota is preparing relevant structures by incorporating necessary provisions in its business continuity plan (BCP) and conducting joint training with the local governments.

Details of the major support items are described below. Other support items agreed with individual local governments include provision of designated shelter facilities.

Details of the Major Support Items

1. Rescue and relief in a disaster
2. Provide temporary evacuation facilities to local residents
3. Provide food, drinking water, and daily necessities for distribution through local governments (local residents)
4. Support cargo handling at municipal relief supply facilities
5. Provide space necessary for restoration of local infrastructure (water supply and drainage, roads, etc.)
6. Employee participation in local recovery activities

Building a Disaster-resilient Supply Chain with Suppliers

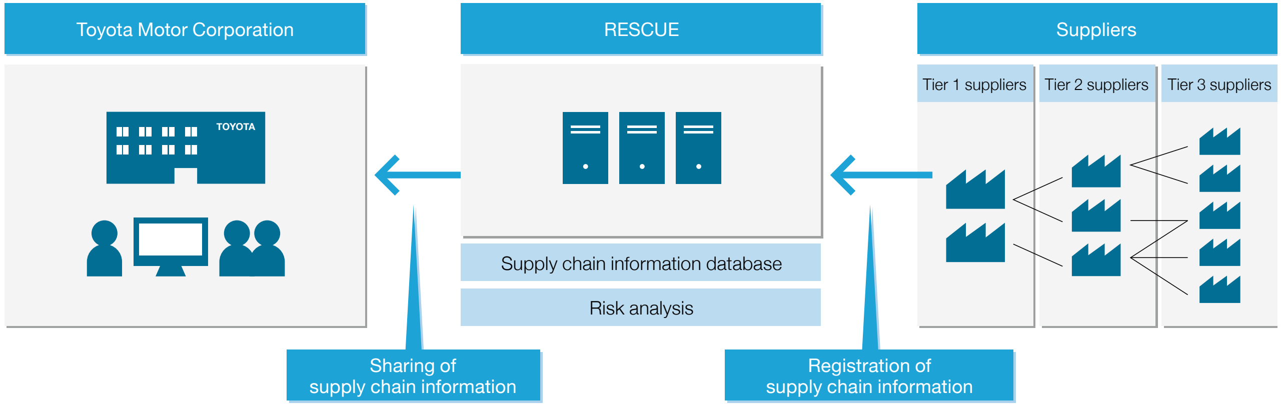
Toyota has provided recovery support in accordance with the following priorities: (1) Humanitarian aid; (2) Early recovery of the affected area; (3) Restoration of Toyota's operations and production. Since the Great East Japan Earthquake, we have worked with suppliers in each country and region to build a disaster-resilient supply chain by sharing supply chain information and setting up measures for prompt initial action and early recovery.

In sharing supply chain information in Japan, Toyota receives highly confidential information from suppliers and build up a database, RESCUE (REinforce Supply Chain Under Emergency) system, based on the concept of protecting Japanese *monozukuri* (manufacturing). Under strict protection of suppliers' confidential information, Toyota conducts regular training with suppliers to utilize the system in case of a disaster. It was also utilized in the Kumamoto Earthquake in April 2016, Northern Osaka Earthquake (May 2018), and heavy rain disaster in western Japan (June 2018).

This system has been standardized and shared with other companies through the Japan Automobile Manufacturers Association, helping thus to build a disaster-resilient supply chain.

Toyota is implementing equivalent initiatives with suppliers in each country and region overseas.

RESCUE System Storing Supply Chain Information


Toyota Motor Corporation
TOYOTA
RESCUE
Supply chain information database
Risk analysis
Suppliers
Tier 1 suppliers
Tier 2 suppliers
Tier 3 suppliers
Sharing of supply chain information
Registration of supply chain information