Risk Management

JR-West Group's approach to risk management

Even as the social environment undergoes significant change, the JR-West Group continues to ensure that it lives up to society's trust. Towards that end, we maintain a Risk Management Committee, which is chaired by the president and includes executive directors and other officers, to identify risks and critical matters that could have a major impact on Group operation, as well as to inspect and evaluate the Group's risk management mechanisms and systems.

Additionally, each group company works to identify and mitigate risks that could significantly impact that company's operations, with the active involvement of management.

Initiatives are formulated in line with the ISO 31000 international standard for risk management as we work to develop a system for proper risk management that encompasses all of the Group's business activities.

Head of operations;
Vice President, Representative Director, and Executive Officer
Shoji Kurasaka

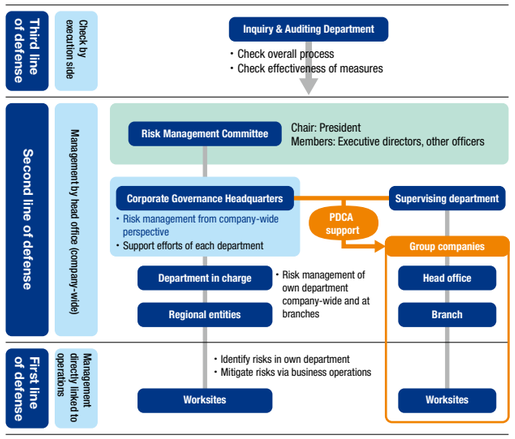
Risk management system

At JR-West, we have a risk management system in place within our PDCA cycle, which utilizes the three lines of defense.

The first and most basic line of defense is the autonomous risk management performed at each operational/service worksite.

The second line of defense is the staff departments, which oversee the operational/service worksites and who are responsible for pursuing risk management via on-site guidance, support, and other means.

The third line of defense is the internal auditing department, which performs independent and objective reviews of overall processes and confirms the effectiveness of measures.



Compliance initiatives

See page 56.

Crisis management

- In order to ensure a swift and appropriate first response in the face of a diverse array of possible crisis situations, such as natural disasters, infectious diseases, or terrorism, we have developed systematized rules and manuals, established an emergency information communication system, conduct regular drills, and undertake various other measures.
- We have created a business continuity plan (BCP), which ensures that we can flexibly adapt our business execution structure to the level of crisis faced.

■ First-response training for a large-scale disaster

Information Security

JR-West Group's approach to information security

In order to protect the JR-West Group's information assets from various threats, we have established and adhere to the JR-West Group Information Security Policy. We declare that we will leverage information-sharing and cooperation among group companies to facilitate the implementation of ongoing, group-wide information security measures.

In recent years, the Japanese government has called for stronger cybersecurity as part of its national policy. As an entity responsible for key infrastructure, we treat information security as a business priority, looking for ways to address the increasing vulnerabilities that accompany the expansion in telework and digital transformation, the increasing sophistication of cyberattacks, and the increasing number of threats.

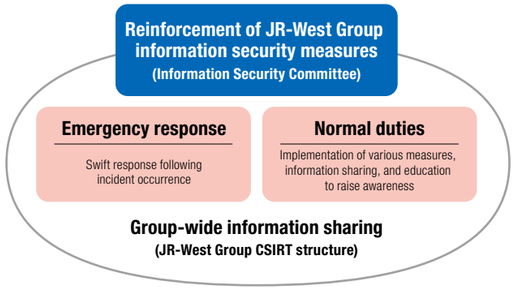
Head of operations;
Director and Executive Officer;
Senior General Manager of Digital Solutions Headquarters
Hideo Okuda

Information security systems

At JR-West, we have established an Information Security Committee, which shares organization-wide risks with management, deliberates on the direction security measures should take, and fosters shared awareness with management at group companies for the sake of achieving these measures.

We have also established the JR-West Group CSIRT*, which exists as a cross-functional organization within the Group, to focus on preventing security incidents from occurring and, if they do occur, keeping them contained.

*CSIRT: Computer Security Incident Response Team. An organization responsible for handling computer security-related incidents.



Improving crisis response capacity

- As part of regular education, we hold information security education for all employees and training sessions for senior management. Participants who complete prescribed training are certified as information security leaders, which is an independent, in-house qualification.
- As part of emergency-response education, we hold incident-response training for CSIRT members and targeted email attack training for employees, including those at group companies.
- We foster deeper cooperation with governmental bodies through temporary placement of personnel within the IPA (Information Technology Promotion Agency) Industrial Cyber Security Center of Excellence and participation in collaborative, critical infrastructure-focused training with the NISC (National Center of Incident Readiness and Strategy for Cybersecurity).

Establishing the PDCA cycle

We maintain guidelines for specific security standards that must be followed, and we update them in response to technological trends and past incidents. Based on these, we conduct self-inspections of the IT environment at JR-West and group companies each year to strengthen security measures on an ongoing basis.