| JFR Sustainability Management | JFR Materiality Issues | Realization of Decarbonized Society | Promotion of Circular Economy | Management of the Entire Supply Chain | Promotion of Diversity & Inclusion | Realization of Work-Life Integration | Realization of Customers Healthy/Safe/Secure life | Coexistence with Local Communities | Sustainability Initiatives of Operating Companies | Risk Management | External Recognition | Sustainability Data |

→ Information Security

Risk Management

The Group's View and System of Risk Management

The Group defines risk as "uncertainty that affects the achievement of business management goals and has both a positive side and a negative side." We believe a company will grow in a sustainable way if the positive side and the negative side of risk are addressed properly. In our risk management system, we have formed the Risk Management Committee, which is chaired by the President and Representative Executive Officer and comprises Executive Officers and other members, as an advisory body to the President and Representative Executive Officer. The committee has a secretariat headed by an officer in charge of risk management.

The secretariat shares important matters decided by the committee with operating companies to promote enterprise risk management (ERM).
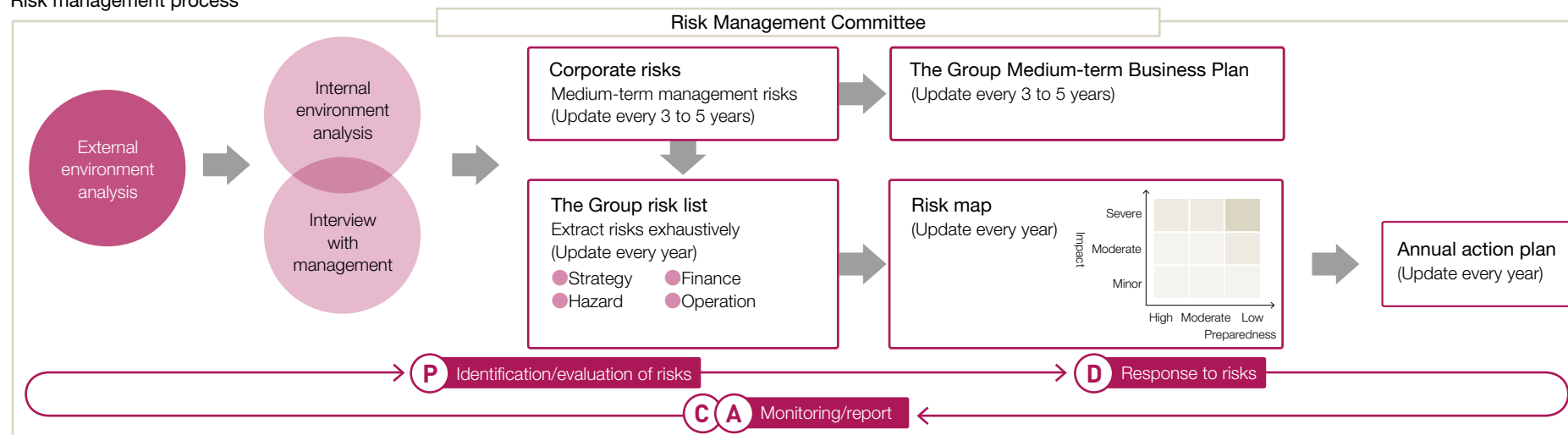
We position risk as the starting point of strategy and link risk with strategy so that we can enhance corporate value through risk management.

Risk Management Process

The Group promotes risk management through the process below. Specifically, based on external and internal environment analyses and the recognition of the management team including Directors and people responsible for practical operations, we strive not to omit any important risks for the Group. Extremely important risks in the Group's management over the medium term are positioned as "corporate risks," which are the starting point of the Group's Medium-term Business Plan.

Annual risks identified based on the "corporate risks" are listed in the "Group risk list" and evaluated using a "risk map" and we implement measures to address them in order of priority.

Risk management process

→ Information Security

Corporate Risk List

The following list summarizes the impact of the fourteen "corporate risks" on the Group and the measures against them. The measures are linked to the Medium-term Business Plan and we periodically manage their progress.

Category	Item	Impact	Outlook for next fiscal year	Negative side	Positive side	Measures
Strategy risk	Decline of existing business models	Very severe	↑	●Decreased vitality of the entire Group due to weak performance of core businesses	●Regrowth by radical change of core business model	●Increasing store appeal and asset value of urban large-scale stores by enhancing content appeal, fusing with digital technologies, and increasing environmental value
	Advanced sustainability management	Very severe	↑	●Defection of investors and shareholders, lower rating due to delay in taking action	●Sustainable growth by steady action	●Realizing Well-Being Life by promoting 7 materiality issues including "realization of decarbonized society"
	Response to increasingly accelerated digitalization	Very severe	↑	●Sluggish growth of the entire Group ●Declining competitiveness	●Changing the business models of existing businesses ●Renewing awareness of real connection with people	●Changing business models through OMO ●Improving communication physically and digitally ●Changing operations by digitalization
	Urban decentralization (Rebalancing between urban and rural areas)	Severe	↗	●Decline in conventional urban commercial facilities' ability to attract customers	●Business in response to urban decentralization	●Strengthening epidemic prevention and contactless services in urban stores ●Real estate development in urban and semi-urban areas for not only commercial but mixed use
	Changes in consumer behavior after COVID-19	Severe	↗	●Poor performance due to failure to meet consumer needs	●New market development	●Rightsizing commodities ●Enhancing customer satisfaction through OMO ●Strengthening art, culture and ethical products
	Accelerated reorganization and M&A beyond industry boundaries	Severe	↗	●Hostile takeover of the Group	●Overhaul of business portfolio ●Corporate growth using M&A	●Increasing resilience of business portfolio ●Creating new businesses by M&A and business alliance with other companies
	Work styles in new normal era, progress of HR/organization reforms	Severe	↗	●Talent drain ●Losing the war for talent	●Creating innovation by changing corporate culture	●Strengthening mid-career employment ●Improving flexibility in work styles ●Changing to sustainable organization
	Accelerated income polarization	Severe	↗	●Poor performance due to shrinkage of volume market	●Emergence of new affluent markets	●Rightsizing products/services in volume price ranges ●Deeply cultivating affluent markets with diverse approaches
	Changes in customers, particularly low birthrate / longevity	Severe	→	●Shrinkage of domestic markets	●Expansion of senior markets	●Deeply cultivating high quality children's markets ●Creating safe and secure store environment ●Strengthening art/culture/wellness
	Uncertainty about non-Japanese market	Severe	→	●Prolonged significant decrease in inbound sales	●Acquisition of foreign demand with new approach	●Reviewing inbound strategy ●Strengthening cross-border EC and live commerce
Finance risk	Increasing importance of financing management	Severe	→	●Business failure due to lack of funds ●Sluggish growth due to financing on unfavorable terms	●Business development by investing in growth areas and securing funds	●Centralizing the Group's financing and improving fund efficiency ●Diversifying financing methods
	Need for cost structure that can respond to environmental changes	Very severe	↗	●Business survival crisis ●Delay in performance recovery	●Business portfolio realignment ●Investment in growth businesses	●Cost reduction by business model reform ●Narrowing down business base
Hazard risk	Frequent natural disasters / epidemics	Very severe	→	●Damage to the lives of customers and employees ●Business continuity crisis	●Contribution to ensuring the safety and security of local communities	●Developing manuals for "business continuity" and "response to infections" ●Continuously conducting BCP training
	Increasing importance of information security	Severe	↗	●Loss of social credibility and operating loss due to the leakage of important information ●Delay/stagnation of operations	●Promotion of smooth DX (digital transformation)	●Developing Information Security Policy and IT Governance Policy ●Promoting transition to cloud-based systems ●Improving information literacy through education/training

Information Security

With increasingly sophisticated cyber attacks, the Group promotes security measures based on the NIST[*1] Cyber Security Framework to restore as early as possible premised on the assumption that it is impossible to completely prevent from being hacked and that the Group is subject to attack.

CSIRT[*2] was established in the Company and the Company works with people responsible for information security management of each company in the Group to develop manuals in preparation for incidents and provide incident response training to strengthen the security management system of the entire Group.

The IT Governance Policy and Rules formulated in 2020 define compliance with the Information Security Policy as one of the Group's key measures. As such measures, we continuously provide e-learning programs and targeted attack email training for all employees to ensure employees' compliance with and raise their awareness of information security.

In addition, in light of environmental changes including the penetration of telework and the expansion of cloud services, we are working to introduce the systems that isolate and restore devices for business use at the time of incident and visualize and control unauthorized cloud services. We will take information security measures that are safe and not bound by workplaces. And at the same time, we will put in place systems that promptly analyze and respond to cyber attacks and update them all the time to prevent any omissions in the measures.

*1 National Institute of Standards and Technology
*2 Computer Security Incident Response Team