Chapter 11
Risk Management

Yoshinari Hayashi and Katsuyuki Kamei

Abstract Risk management consists of a series of actions to list out all possible risks, evaluate their influences, and reduce or avoid the losses. We hear the term "risk management" in a number of fields including finance, corporate management, safety of machine systems, accident prevention, and natural disasters. The fields, however, have different concepts and understanding of its controllability associated with the term. In most fields, risk is pure risk that can only produce negative effects, but in some cases, evaluating speculative risk with both negative and positive effects is important.

Keywords Pure risk · Risk assessment · Risk treatment · Speculative risk

11.1 What Is Risk Management?

11.1.1 Nature of Risk Management

Frequently quoted in other chapters, the 2009 international standards of risk management, ISO 31000:2009 "Risk Management – Principles and Guideline," defines risk as "the effect of uncertainty on objectives" and risk management as "coordinated activities to direct and control an organization with regard to risk" (ISO 2009). The concept of risk has more than one tracks of development. The first is a financial approach centered around business administration and insurance, and the second is safety engineering oriented. Further, there are the third and fourth approaches that are oriented along science of disaster management and along law. The concept of risk management is spreading among, not only corporations, but a number of fields including nation, administration, local societies, educational institutes, medical institutes, homes, and individuals.

Y. Hayashi (✉) · K. Kamei
Faculty of Societal Safety Sciences, Kansai University, Takatsuki, Osaka, Japan
e-mail: yhayashi@kansai-u.ac.jp

S. Abe et al. (eds.), *Science of Societal Safety*, Trust: Interdisciplinary Perspectives 2,
https://doi.org/10.1007/978-981-13-2775-9_11

J. H. Fayol of France first pointed out the importance of risk management in business administration. He pointed to "security function" as a corporate activity and defined it as "protection of resources and employees" in his 1916 paper *Administration Industrielle et Générale* (Fayol 1916). Since this paper, risk management has meant management, know-how, systems, and countermeasures to overcome risk.

On the other hand, in the USA, insurance management-type risk management turned into the standard in the 1950s. The 1956 Gallagher paper "Risk Management: New Phase of Cost Control" is from that time. The paper pointed out "how much cost to spend on safety and risk management" (Gallagher 1956), an angle still in practice today. Then in the 1970s to the 1980s, American insurance management-type risk management theories made their ways into Japan.

In the 1960s, safety engineering fields in Japan started to take on risk management-type methods (Hollnagel 2014). The main reason was, at the time, machine systems quickly turned complex and they needed ways to analyze risks. For actual engineering systems, engineers developed analysis methods, for example, fault tree analysis, that estimates the probability of functional failure based on causal events and reliability data, and event tree analysis that analyzes event progress of systems.

After the outbreak of the TMI accident in the USA in 1979, methods of risk management have shown further development since the first half of the 1980s. Analyses of the TMI accident showed that human factors and human error pose serious effects on system safety. Thus, risk assessment and accident analysis started to involve people and organizations, in addition to technical and engineering aspects of machine systems, into the overall system evaluation.

Recent machine systems have complex functions intertwined with one another and, at the same time, feature distributed functions over wide areas on the Internet. The advancement of technologies in mechanical and information communication pushed for more researches in developing risk management methods, and risk management now plays a central role in resilience engineering.

Risk management originally started and developed in fields of man-made disasters; thus, its history in dealing with natural disasters is relatively new. It is difficult for human to control natural phenomena that cause natural disasters. Also, earthquakes and volcano eruptions have low frequencies of occurrence; thus, their mechanisms, needed for evaluating external force magnitudes, were not well clarified even in the 1980s. For this reason, in disaster prevention to prepare against natural disasters, it was common to set the standards to the maximum in the past records. This method only works to prevent the same disaster again and is not along the line of risk management. Risk management against natural disasters spread in Japan after the 1995 Great Hanshin-Awaji Earthquake (Okada 2004).

In case of earthquake disasters, for example, performing risk management takes damage estimation with the following procedure:

1. Establish source model for the earthquake to analyze.
2. Estimate the strength of ground motion or seismic intensity at each point of interest.

3. Estimate the magnitude of damage caused by different strengths of ground motion.
4. Collect damage estimates at locations of interest and show them on a map.

The development of geoscience theories since the 1970s and the accumulation of measurement data allowed us to reach a reasonable source model of earthquakes in item (1). Rapid advancement of theories and simulation technology of earthquake wave propagation have also made estimating spatial distribution of earthquake motion intensities in (2) based on source models in (1). A number of practical empirical equations have been proposed to relate the damage rate of buildings with earthquake movement intensities. Therefore, multiplying damage rate estimated to the number of buildings or the number of people living in specific areas gives us the magnitude of damage needed for (3). Collecting the results of (3) leads to (4) that are in fact published in the forms of hazard maps or damage estimation. Local organizations and corporation have started to prepare against disasters in risk management styles based on damage estimates from (4).

Today, what risk management means have a great variety depending on who is carrying them out against which risk and differences in the concept of management. In the field of corporate risk management, the framework of enterprise risk management (ERM) announced in 2004 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and revised in 2016 is widely accepted (COSO 2004, 2017).

11.1.2 Concept of Risk

Risk, in the past, had been defined as "combination of the consequences of an event and the associated likelihood of occurrence" (ISO/IEC Guide 73:2002) or "combination of the probability of occurrence of harm and the severity of that harm" (ISO/IEC Guide 51:1999). ISO 31000:2009 and ISO Guide 73:2009 in 2009 added to these definitions "the effect of uncertainty on objectives." In the background of change in the definition of risk is the modern concept of risk management to deal not only with risks that cause negative effects, but also with risks with positive effect when decisions to take the risks are made.

Traditional risk management theory divides risk into pure risk and speculative risk. As Table 11.1 shows, the former is "loss only risk" like damages from natural disasters or accidents by chance. The latter, on the other hand, is loss or gain with a risk that may result in loss with changes in corporate activities or operational environment but can also lead to profit by preventing the generation of loss, i.e., the risk in case of "risk taking." Table 11.1 summarizes these risks.

Table 11.1 Pure risk and speculative risk

Pure risk: objectives of risk treatment	Loss-only risk
	Risks that only produce negative effects (loss)
	Operational risk
	Accident, disaster, liability
	Objectives related to protection, prevention, and insurance
Speculative risk: objectives of risk taking	Loss or gain risk
	Possibility of negative effect (loss) and positive effect (gain)
	Business risk, strategic risk
	Uncertainty with success or failure of new business, capital investment, new product development, funding, M&A, and so on
	Objectives of decisions about business chances and operational strategies

11.1.3 Elements of Risk

The theory of risk management mainly discusses safety management and insurance management. It takes risk as possibility of accident occurrence and covers such elements like (1) hazard, circumstances and conditions that affect accident occurrence; (2) exposure, people and objects that are exposed to risk; (3) risk, possibility of accident occurrence; (5) crisis, nearing of accident breakout and persistence of accident consequences; and (6) loss.

As we discussed in Chap. 1, the term "hazard" means latent source (generation source or characteristics) of harm. The term hazard, however, has different nuances depending on the field. Young and Tippins explained hazard as "probability of generating loss or environment and conditions that elevate the degree of loss." They also explain its synonym risk factor to mean "it is a synonym of hazard but it also includes investment risk with possibly positive outcome in addition to negative outcome" (Young and Tippins 2000). In applying risk management, we need to clarify which of these elements we place in the center of our work.

11.1.4 Process of Risk Management

ISO 31000 stands out in clarifying the term definitions and showing risk management processes that are applicable to all types of organizations. Processes of risk management takes the form of (a) communication and consultation and (b) monitoring and review interacting with each other at each stage of (1) establishing the context, (2) risk assessment, or (3) risk treatment.

11.1.5 Establishing the Context

ISO 31000 places "context establishment" at the first stage of risk management process. In establishing the context, the process defines external and internal factors to consider for managing risks and sets the applicable range and risk criteria along the risk management guideline. For the best risk management, an organization first has to recognize its context. That is to understand (1) the situations and environment where the organization stands, (2) resources the organization owns, and (3) its mission and strategies to carry out.

11.2 Risk Assessment

11.2.1 Risk Assessment

The second stage of risk management, according to ISO 31000, is "risk assessment." Risk assessment analyzes the frequency of risk outbreaks and levels of influence. At the same time, based on risk criteria, it evaluates whether to accept or avoid risks and what the significant risks are and prioritizes responses to risks. Risk criteria here are cost requirement for risk responses, upper limits of resources for risk exposures, possible benefits for accepting risks, regulatory constraints and requirements, impact on the environment, and expectations by the stakeholders. Risk assessment uses matrices and risk maps showing relations of risk frequencies and effects.

11.2.2 Risk Identification

ISO 31000 defines that the first stage of risk assessment is risk identification to find and recognize risks. Risk identification takes risk-sensitive minds to clarify the following points:

1. List out exposures, that is, to check what human and physical resources the organization has
2. Clarify what accidents may take place, i.e., human risks, physical risks, liability risks, and risks in cost
3. Find what forms of losses are expected like human loss, physical loss, non-recoverable receivable, loss of profit, or liability for damage compensation

A number of methods are available for identifying risks: (a) field investigation, (b) interview, (c) discussion sessions, (d) checklist, (e) questionnaire, and (f) flowchart.

11.2.3 Risk Analysis and Evaluation

ISO 31000 states the second stage of risk assessment is risk analysis. The third stage that follows is risk evaluation to estimate the effect of risk. In these stages, we have to assess probabilities of accident occurrences or their frequencies and the sizes of losses in case the accidents take place, i.e., the magnitude or influence of accidents. For each specific risk, the stages analyze and evaluate the probability or frequency of the risk developing into a real accident and what influence it makes as a result.

On the other hand, risk maps visualize the risks based on the results of identification and evaluation. For a risk map, a visualization for anyone to recognize the risks is important.

ISO defines risk analysis as a "process to comprehend the nature of risk and to determine the level of risk" and risk evaluation as a "process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable." Control self-assessment (CSA) is a method for risk analysis and evaluation.

11.3 Risk Treatment

The phrase "risk treatment" means deciding the response to risk or selecting the method of risk handling. It is a decision-making process for an organization to select the best risk handling method based on set criteria and necessary cost estimates.

Risk treatment decides how to handle the risks identified and evaluated with risk assessment. ISO 31000:2009 defines risk treatment as a process of modifying risks with possibly the following:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision

Risk treatment has two pillars of risk control, to prevent accidents or to take disaster responses and risk finance to prepare funds or applying insurance. There are four methods of risk treatment: (1) avoidance, (2) removal/reduction, (3) redirection/transfer/sharing, and (4) retention/acceptance. Actions to treat a risk that broke out without avoiding it involve reducing it to the extent possible. Then further efforts of transferring the residual risk to others or sharing it takes place. Parts of the risk that escaped redirecting, transferring, or sharing are kept within.

Two ways of risk retention exist: one is passive retention as a result of being unaware of it and the other is active retention with full understanding of the risk. Active risk retention is further separated into one with a priori preparation and one with no preparation, i.e., postponed response. There is advantage in active risk retention with thorough understanding of the risk over passive risk that we recognize for the first time after the exposure to it. ISO 31000 also recommends retaining risks after making decisions to do so based on information.

11.4 Executing Risk Management

11.4.1 Communication: Sharing Understanding about Risk Treatment

Figure 11.1 shows risk communication for corporate operation. The components in the figure show that companies need to share common understanding of (1) what risks the company holds and (2) how to treat such risks among (a) structures within the company and (b) outside stakeholders. Corporate disclosure of risk information means listing problems to handle, operational risks, financial standing, business performance, cash flow analysis, and corporate governance and, so in the financial report, describing "Rules and other systems for managing risks of loss" in the corporate governance report and explaining such matters in the shareholder's meetings.

11.4.2 Coordination: Organizational Structure of Risk Management

ISO 31000 defines risk management as "coordinated activities to direct and control an organization with regards to risk." Coordination in this definition means to

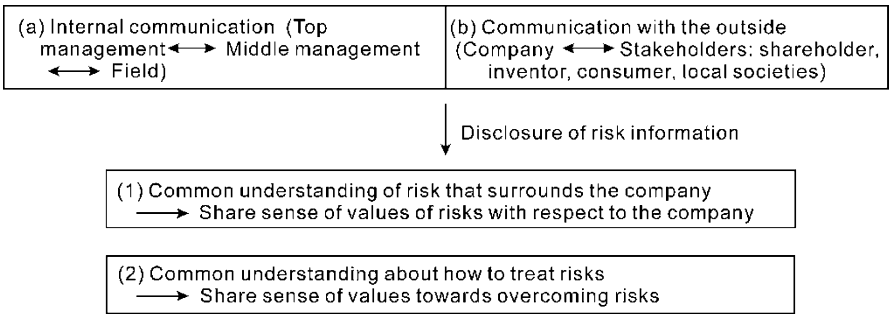

Fig. 11.1 Risk communication for corporations

organize conditions about risk treatment within the organization and to derive the best solution for interests of the stakeholders. Corporations these days commonly establish risk management committees for coordinating risk management. Risks that are unique to departments of production, sales, information processing, and so on are handled within the departments. Risk management committees take on risks that affect multiple departments or the whole companies. Today, risk treatment targets "risk optimization" by minimizing the loss and maximizing the profit. In actual societies, "risk zero" situations with no risk are impossible. Because there are risks that threaten us, we make efforts to overcome them with risk management. The efforts lead to raising corporate values.

References

COSO. (2004). *Enterprise risk management – Integrated framework (executive summary)*. The Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf. Accessed 6 July 2018.

COSO. (2017). *Enterprise risk management – Integrating with strategy and performance (executive summary)*. The Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf. Accessed 6 July 2018.

Fayol, J. H. (1916 [1917]). Administration industrielle et générale, Dunod, Paris. Extracted from *Bulletin de la Societe de l'Industrie Minerale*, fifth series, *10*(3), 5–162.

Gallagher, R. B. (1956). *Risk management: New phase of cost control*. Boston: Harvard Business Review.

Hollnagel, E. (2014). *Safety I and safety II: The past and future of safety management* (1st ed.). Boca Raton: CRC Press.

ISO. (2009). *ISO 31000:2009 risk management – Principles and guidelines*. International Organization for Standardization (revised by 31000:2018).

Okada, N. (2004). Urban diagnosis and integrated disaster risk management. *Journal of Natural Disaster Science, 26*(2), 49–54.

Young, P. C., & Tippins, S. (2000). *Managing business risk: An organization – Wide approach to risk management*. New York: AMACOM.