Journal of Service Science and Management, 2025, 18(6), 432-460
https://www.scirp.org/journal/jssm
ISSN Online: 1940-9907
ISSN Print: 1940-9893

Risks in Services and Their Management

Cengiz Haksever

Department of Information Systems, Analytics, and Supply Chain Management, Norm Brodsky College of Business, Rider University, Lawrenceville, NJ, USA
Email: haksever@rider.edu

How to cite this paper: Haksever, C. (2025). Risks in Services and Their Management. *Journal of Service Science and Management, 18,* 432-460.
https://doi.org/10.4236/jssm.2025.186028

Received: October 4, 2025
Accepted: November 17, 2025
Published: November 20, 2025

Abstract

Risks and risk exposures exist in all services with a wide range of consequences concerning human lives and property. Although there are risks common to most services, each service area has a set of unique risks that need different approaches for their management. This paper reviews risks in services in general and their management. Although ample research publications on risk management in various service industries like healthcare, airlines, airports, air traffic control, banking and finance, and hospitality exist, a literature survey revealed only one journal publication on service risks in general and their management in the literature. The purpose of this paper is to contribute to this neglected area of service management. It provides a brief background on risks for service managers and methods, concepts, and tools to defend their organizations against risks.

Keywords

Risks, Enterprise Risk Management, Vulnerability, Resilience, Robustness, Air Travel

1. Introduction

All service, manufacturing, or extraction industries face a wide variety of risks. Some of these risks are minor, but some pose a significant threat to their survival. Identifying, analyzing, assessing, treating, and managing risks is part of the risk management duty of service managers. This paper focuses on the service sector of the economy, reviews risk concepts, approaches to risk management, and the tools and methods that service managers can use to protect their organizations. There is ample research on risks and their management in specific service industries, such as healthcare, air travel, hospitality, finance and banking, etc. However, the literature survey revealed only one journal publication that focused on services in general (Hollman and Forrest, 1991).

Hollman and Forrest (1991) focused on the risk management concept and its application to service businesses. They characterized risk management as the application of general management concepts and proposed a five-step process to help managers cope with risks of pure loss exposures. In addition, the authors proposed a set of insurance, noninsurance, and financing techniques to treat risks of loss.

The literature survey found two tangentially relevant publications, one by Hollman and Mohammad-Zadek (1984), who described the risk management concept and the process that is used in applying it in small businesses, and a second by Nordin et al. (2011) focusing on services provided by manufacturing companies. The authors of the paper examined the risks for manufacturing companies in extending their goods offerings by the addition of different kinds of services. They also developed a conceptual framework that helps manufacturing managers assess the risks of infusing various services into their offerings of goods.

The literature survey for this paper was conducted between 8/25/2025 and 10/14/2025 using the databases ABI/INFORM Complete, Academic Search Premier, Business Abstracts with Full Text, Business Source Premier, EBSCO Databases, JSTOR, and Health Source: Academic/Nursing Edition, using the keywords risks, enterprise risk management, healthcare, vulnerability, resilience, robustness, air travel, and hospitality industries.

The rest of the paper is organized as follows. Section 2 reviews risks in general and various definitions of risk from the literature. Section 3 discusses risk management and enterprise risk management as two approaches to managing risks in any organization. Section 4 is a review of types of risks in general. Section 5 discusses vulnerability, resilience, and robustness as relevant concepts in risk management. Section 6 reviews methods and tools that can help service managers decrease vulnerability, and increase the resilience and robustness of their organizations. Section 7 presents risks in air travel and their management as an example of risks in an important service industry. Section 8 presents risks and their management in hotels and resorts as another example. Section 9 is where a summary of the paper and conclusions are presented.

2. Risk Definition

This subtitle may give the impression that there is a single definition of risk. However, there is no universally accepted definition of risk among risk researchers or risk management practitioners. "The word 'risk' derives from the early Italian *risicare*, which means 'to dare'" (Wolke, 2017). Risk and risk management scholars have proposed various definitions, some overlapping and others distinct. Before examining examples of risk definitions, it is important to distinguish between two types of risks.

Pure risks are those risks that can only lead to *loss* or no *loss*; there is no possibility of a gain. Pure risks can be insured if insurers are able to predict the potential losses and agree to cover them. Olson & Simkiss (1982) presented a review of fun-

damental concepts that must be recognized to adequately understand risk management: analyze the objectives of risk management, understand the basic nature of risk management, and identify and analyze appropriate alternatives. They also reviewed various financial insurance alternatives to protect the organization against pure risks. *Speculative* risks are those risks that may lead to loss or gain for the risk taker (Williams, 1966; Johnson & Flanigan, 1977; Hollman and Mohammad-Zadek, 1984; Hollman and Forrest, 1991; Wolke, 2017). This distinction seems to be accepted by both risk researchers and practitioners. Pure risks will be the focus in this paper.

The following is a sample of risk definitions from the literature:

- "Risk is the 'possibility of loss or injury' and the degree of probability of such loss" (Kaplan and Garrick, 1981).
- "Risk is "the possibility that bad or good things may happen" (Nason and Livvarcin, 2020).
- "Risk is based on possible damage or the potential loss of a net asset position, with no potential gains to offset it" (Wolke, 2017).
- "Risk equals the expected disutility" (Campbell, 2005).
- "Risk can be defined as "an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives" (Kim, 2017).
- "Risk refers to uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value" (Aven and Renn, 2009).
- "Risk is the potential of gaining or losing something of value" (Stamatis, 2019).
- "Risk is a situation or event where something of human value (including humans themselves) has been put at stake and where the outcome is uncertain" (Rosa, 1998).
- "A common definition of risk includes two dimensions: the probability of occurrence and the associated consequences of a set of hazardous scenarios" (Gardoni and Murphy, 2014).
- "*Risks*, or equally *risk events* (noun), refer to future events with undesirable consequences without specific regard to intent, and hence include accidents and non-accidents" (Pinto and Magpili, 2015).
- "We consider a future activity [interpreted in a wide sense to also cover, for example, natural phenomena], for example, the operation of a system, and define risk in relation to the consequences (effects, implications) of this activity with respect to something that humans value" (Aven et al., 2018, Society for Risk Analysis Glossary).

Risks created by "unknown unknowns" as described by former defense secretary Donald H. Rumsfeld (DoD News Briefing, 2002) should be added to these risk definitions (Kim, 2017). The probability and impact of these events are impossible to know. Some of the events that fit this description include Ebola virus disease (EVD), severe acute respiratory syndrome (SARS), COVID-19, mad cow disease, and the horse meat scandal. Another hard-to-predict, low-probability,

high-impact extreme outlier category of events that are almost impossible to predict are known as "Black Swans" (Taleb et al., 2009). Some examples of black swan events are the "Black Monday" stock market crash of October 19, 1987, the "Dot Com" crash of 2002, and the September 11 terrorist attacks.

For the purposes of this paper, the following definition of risk will be used:

"*Risk is the uncertainty about and severity of the consequences, effects, implications, of an activity, including natural phenomena, with respect to something that humans value.*"

This definition is consistent with Rosa (1998), Aven and Renn (2009), and (Aven et al., 2018, Society for Risk Analysis Glossary).

It should be noted that researchers and practitioners in different sectors of the economy, such as manufacturing, agriculture, mining, finance and banking, air travel, healthcare, hospitality, etc., have developed risk definitions that are appropriate for their sectors. "… each disciplinary literature on risk can similarly be categorized to provide unique epistemological perspectives. As a result, all the disciplines have something valuable to add to our understanding of risk" (Althaus, 2005). Risk definitions for one segment of the service sector, air travel and airports, will be reviewed as an example later in the paper. It should also be noted that types of risks and their relative importance for an organization depend on the specific features of the organization, such as industry characteristics, and services and goods produced (Wolke, 2017).

Regardless of how they may be defined, risks must be managed. There are two major approaches that are commonly used in manufacturing and service organizations: risk management (RM) and enterprise risk management (ERM). The next section will review these approaches.

3. RM and ERM

An early definition of Risk Management (RM) states that it is "the process of planning, organizing, directing, and controlling the resources and activities of an organization so that the possibility of loss or injury is reduced to the lowest possible level at the lowest cost" (Dillon et al., 1984). RM is a process "that identifies loss exposure faced by an organization and selects the most appropriate techniques for treating the loss exposures" (Rejda et al., 2022); as such it focuses on the negative, threats, and failures (Kaplan and Mikes, 2012). The major criticism of RM is that risks are dealt with in "silos", each function of an organization, such as operations, finance, marketing, etc., focusing on and dealing with its own risks (Fraser et al., 2021).

Enterprise risk management (ERM) is advanced RM that deals with all major risks faced by an organization; pure risk, speculative risk, strategic risk, operational risk, and financial risk are the major risk categories (Rejda et al., 2022). Some authors consider more categories of risks managers must deal with, such as market, credit, legal, and reputation risks (Crouhy et al., 2023). ERM is also referred to as "holistic risk management" (Schneier and Miccolis, 1998). In other

words, ERM must be aligned with the strategy and mission of an organization (Hardy, 2015). Nocco and Stulz (2022) reviewed the benefits of ERM as creating value for shareholders and examined the practical issues in the implementation of ERM. Like the lack of a universally accepted risk definition, many researchers and practitioners have offered different definitions of ERM (See Bromiley et al., 2015). The following is a small sample of ERM definitions from the risk literature:

ERM is a structured and disciplined approach to help management understand and manage uncertainties and encompasses all business risks using an integrated and holistic approach (Sobel and Reding, 2004).

Enterprise Risk Management (ERM) "is a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio." RIMS (The Risk Management Society) (2025).

"Enterprise risk management (ERM) is a methodology that looks at risk management strategically from the perspective of the entire firm or organization. It is a top-down strategy that aims to identify, assess, and prepare for potential losses, dangers, hazards, and other potentials for harm that may interfere with an organization's operations and objectives and/or lead to losses" (Hayes, 2025).

"The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value." (COSO, 2020) (COSO is a private sector initiative sponsored by five accounting- and auditing-related associations).

Various professional organizations and researchers have proposed frameworks and conceptual models for ERM. Three well-known frameworks by professional organizations are by COSO (2017), International Organization for Standardization (ISO, 2018), and CAS (2003) (See Sidebar, ERM Frameworks by three professional Societies). These frameworks and models have been designed for business organizations in general; they are applicable to both service and manufacturing organizations. However, none of them is considered to be a "one size fits all" type of model; each organization is likely to make modifications, depending on the services or goods (See the **Appendix Notes**).

ERM and its implementations have been criticized in the literature. Bromiley et al. (2015) identify limitations and gaps in ERM implementations that management scholars are best equipped to address. Paape and Speklé (2012) point out that their research found that the COSO ERM framework does not contribute to risk management effectiveness. Similarly, Fraser et al. (2024) provided a review of literature investigating "why many organizations fail or flounder in their attempts to implement ERM." Horvey and Odei-Mensah (2023) present a comprehensive literature review on the measurements and performance of ERM and conclude that, despite mixed findings on ERM and firm performance in the literature, they have found enough evidence that ERM positively affects firms' performance and shareholders' value. See also a literature review by Anton and Nucu (2020) for ERM adoption, determinants of ERM implementation, and the effects of ERM

adoption (See the **Appendix Notes**).

4. Risk Types

All ERM frameworks and models in the literature require the identification and understanding of the risks an organization deals with. Mishra et al. (2019) identify four general categories of risks: strategic, operational, financial, and hazard. Kaplan and Mike (2012) identify three risk categories: preventable, strategy, and external. Francis (2019) provides a more comprehensive list of risks: market and financial risk, credit risk, physical assets risk, operational risk (including crime risk, technology risk, cyber risk, regulatory risk, people risk, legal risk, model risk, data risk, reputational risk, project risk, strategic risk, and supply chain risk). Damali et al. (2021) developed "a comprehensive model of the risks of customer participation in service delivery, integrating research from the marketing, operations and supply chain management, strategy, and information technology fields." Specific risk types in airline operations, air traffic control, and airport management will be discussed later in the paper.

5. Relevant Concepts Related to Risk Management

Any discussion of risks and their management inevitably includes three relevant concepts: vulnerability, resilience, and robustness because of their close relationships (Scholz et al., 2012; Haimes, 2009; Aven, 2011; Zheng et al., 2021; Neuvel et al., 2015; Mentges et al., 2023; Brand and Jax, 2007). Scholz et al. (2012) show how these terms can be consistently defined based on a decision-theoretic, verbal, and formal definition. Any organization using some kind of risk management framework must deal with these concepts and make use of them for risk management and protection of an organization against various risks. Although there are a few other concepts relevant to risk management, such as redundancy in systems (e.g., backup generators), flexibility, reliability, and adaptiveness, the following discussion will focus only on the three concepts listed. As in the definition of risk, various researchers offer a variety of different definitions and interpretations of the three concepts.

5.1. Vulnerability

Merriam-Webster (MW, 2025) defines "vulnerable" as "capable of being physically or emotionally wounded: open to attack or damage: assailable". According to the Cambridge Dictionary (CD, 2025), vulnerability is "the quality of being vulnerable (=able to be easily hurt, influenced, or attacked), or something that is vulnerable." Clearly, any vulnerable organization is at risk and susceptible to loss of lives and/or damage to property.

Vulnerability, resilience, and robustness are frequently researched subjects in risk theory, many fields of natural science, risk management, and business management. Gallopín (2006) offers a perspective to identify and analyze relations among vulnerability, resilience, and adaptive capacity in socio-ecological systems

and "specification of the terms to develop a shared conceptual framework for the natural and social dimensions of global change." McEntire (2011) suggests that vulnerability is related to both liabilities and capabilities that influence the impact of a disaster and reviews four methods for addressing vulnerability. Neuvel et al. (2015) proposed vulnerability reduction strategies for land use planning projects in the Netherlands.

Adger (2006) defines vulnerability as a state of "susceptibility to harm from exposure to stresses associated with environmental and social change and from the absence of capacity to adapt" and identifies challenges to vulnerability research as developing robust measures and incorporating diverse methods for including perceptions of risk and vulnerability. Based on reference frameworks in classical statistical physics, Gheorghe and Vamanu (2004) develop a method to diagnose the current vulnerability of a complex system, as well as to dynamically monitor the time-evolvement of the vulnerability.

Berkes (2007) explored how resilience thinking helps deal with uncertainty and change and discusses how building resilience reduces vulnerability. Aven (2011) points out the inconsistencies in the definitions of risk, vulnerability, and resilience and proposes a framework in which all three concepts incorporate the uncertainty (probability) dimension. Scholz et al. (2012) identify two types of vulnerability: static and dynamic. When the vulnerability of a system is viewed at a certain point in time, it is static vulnerability, and it equals risk. Dynamic is when vulnerability is considered over a period.

Leino et al. (2024) "examine multifactor vulnerability and balanced centricity (beyond customer-centricity) in value creation and value cocreation during disruptive shocks." Fleming (1998) developed a model to offer a framework for managers to help them conduct an analysis of their organization's vulnerability and to take appropriate countermeasures to contain the risks arising from terrorism. Nyanchama (2005) provides insight into defining and implementing effective vulnerability management programs as part of information security management.

Kamalipoor et al. (2023) conducted a bibliometric analysis of vulnerability reduction in technology-based business research and considered four strategies for vulnerability reduction. Kubacki et al. (2020) proposed an integrative framework for vulnerability analysis in social marketing systems by identifying the relationships among power, power asymmetry, vulnerability, and resilience. Bongiovanni and Newton (2019) examined the ways modern international airports can create their own security problems by adopting practices, attitudes, and behaviors that could increase their overall level of vulnerability.

5.2. Resilience

Hollings (1973) was the first to introduce the concept of resilience in ecological systems. This work has had significant impact in the fields of ecology, environmental management, ecological economics and the impact of global change on the lives of humans. He stated that "Resilience determines the persistence of rela-

tionships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters and still persist." "Improving a system's resilience offers significant advantages in managing risk; improving the resilience of a system constitutes an integral part of the risk management process" (Haimes, 2009).

Today, the concept of resilience has been discussed in relation to and applied to many systems. Ecologists make a distinction between engineering and ecological resilience. Levin and Lubchenco (2008) define engineering resilience as "the rate at which a system returns to a single steady or cyclic state following a perturbation" and ecological resilience as "the amount of change or disruption that is required to transform a system from being maintained by one set of mutually reinforcing processes and structures to a different set of processes and structures." Interestingly, these researchers do not make any distinction between resilience and robustness. The focus of this paper will be on engineering resilience relating to all service systems.

Kruk et al. (2015) define healthcare resilience as "the capacity of health actors, institutions, and populations to prepare for and effectively respond to crises; maintain core functions when a crisis hits; and, informed by lessons learned during the crisis, reorganize if conditions require it." Halekotte et al. (2025) identify three understandings of resilience in human-made and natural systems as a process, an outcome, and a capacity, and suggest that only resilience should be understood as a capacity. With reference to supply chains, Christopher and Peck (2004) and Melnyk et al. (2014) state that resilience must be designed into the system. Furthermore, Melnyk et al. (2014) identify two critical capacities of a resilient system: "the capacity for resistance and the capacity for recovery." The first, resistance, defines a system's ability to delay a disruption and reduce the impact once the disruption occurs. The second, recovery, defines the ability to recover from a disruption.

Tasic et al. (2020) developed a multilevel approach to design a framework with which an organization can self-assess its crisis preparedness and response capacity and thus enhance resilience. Tortorella et al. (2023) investigated the relationship between soft lean practices implementation and organizational resilience development in the service sector. Barasa et al. (2018) conducted a review of empirical literature from both the health and other sectors on organizational resilience. They found that the resilience of organizations was influenced by a set of factors, including material resources, preparedness, information management, and redundancy. Hall et al. (2023) identify research approaches and issues in relation to three types of resilience: engineering, ecological, and socio-ecological resilience. The authors provide a synthesis of the core elements of each resilience approach and their implications for hospitality and tourism. O'Connor et al. (2025) performed a bibliometric analysis to examine existing literature on hospitality and tourism small and medium enterprises (SMEs) and their resilience.

Vainieri et al. (2024) studied the definition and operationalization of resilience

in health system performance assessments in European Union countries. They examined resilience and how it was defined and operationalized into key performance indicators in European Union countries. Leino et al. (2024) propose a framework of balanced centricity and service system resilience for service sustainability. Wandelt et al. (2025) developed a novel airport resilience measure, the Global Airport Resilience Index (GARI). Through interviews with international health systems experts, Paschoalotto et al. (2023) found that the COVID-19 pandemic did modify experts' views on various aspects of health system resilience.

Walker (2020) presented an interesting view of what resilience *is* and is *not*: "The simplest definition of resilience is the ability to cope with shocks and to keep functioning in much the same kind of way… Resilience is about learning *how* to change in order not to *be* changed." Walker (2020) also states that "resilience is not always good and desirable. Evil dictatorships, salinized landscapes, and psychotic states in people can be very resilient. The problem in such cases is to know how to reduce their resilience." Gallopín (2006) identifies and analyzes the conceptual relations among vulnerability, resilience, and adaptive capacity within socio-ecological systems.

5.3. Robustness

Like resilience, robustness is an important concept both in engineering and in some other sciences including medicine, ecology, biology, and hydrology. In engineering, robustness is applied to the design of goods and manufacturing processes. Japanese quality expert Professor Genichi Taguchi is credited with developing methods for both (Taguchi, 1986; Taguchi and Clausing, 1990; Taguchi et al., 2005). Taguchi (1986) defined robustness as "the state where the technology, product, or process performance is minimally sensitive to factors causing variability (either in the manufacturing or the user's environment) and at the lowest unit manufacturing cost." In other words, a robust product or process will not deviate from its target design performance specifications because of factors in the environment or in use that may cause variability.

Weiss and Goldberg (2019) show how robust processes reduce variability in service systems and achieve customer satisfaction. Scholz et al. (2012) state that robustness can be seen as an antonym of vulnerability. Stewart (2003) introduced a framework based on the three T's of task, treatment, and tangibles for designing a robust service encounter for improved quality.

5.4. Bringing the Three Together

It should be clear from the above discussion that vulnerability, resilience, and robustness are closely related and play critical roles in service risk management. Strategies and tools for reducing vulnerability, and increasing the resilience and robustness of service systems should be deployed for a successful defense of any service organization against risks. Identifying risks and reducing, avoiding, or

transferring them whenever possible should be the first step in reducing vulnerability and increasing the resilience and robustness of service systems. Insurance against pure risks is one way to transfer some risks to other entities. Investing in redundant equipment such as emergency generators for hospitals, hospitality establishments, and airports helps increase the resilience of these organizations. Using multiple suppliers (for food, supplies, components, and parts) for airlines, hospitals, and hotels also decreases vulnerability and increases resilience. Investments in state-of-the-art information systems and software against cyber-attacks are crucial for risk management. Designing robust and flexible processes, and continuously monitoring economic, political, climatic events, threats, and emerging trends should be part of preparedness for risk events.

6. Tools and Methods

6.1. Poka-Yoke (Error-Proofing)

Tools and methods, mostly from manufacturing management, should be utilized for reducing vulnerability and increasing the resilience and robustness of service systems for effective and efficient risk management. One of the most useful and widely used tools in manufacturing is poka-yoke, also known as fail-safe, error proofing, or mistake proofing, a method that was developed by the Japanese quality expert Shigeo Shingo (1986).

Shingo (1986) developed this method for manufacturing. In manufacturing processes, it utilizes an automatic device or method which makes it impossible for an error to occur or alerts the operator and stops the process so that the error can be corrected. A simple example of error proofing in recycling waste is color-coding trash bins to make separating materials easier. In product design, parts or sub-assemblies are designed so that they can be assembled in only one, the correct way (Dvorak, 1998; Grout, 2006). Another example is SIM cards; they have been designed with a notch so that they can be inserted into a cell phone in only one way. Stewart and Melnyk (2000) introduce the method, implementation steps, and metrics of poka-yoke for manufacturing systems through four building blocks.

Despite its manufacturing origin, poka-yoke has been recommended and applied in improving many services. Chase and Stewart (1994) focused on the application of poka-yoke in services. The same authors provided detailed coverage of the technique in their book for both manufacturing and services (Chase and Stewart, 1995). Stewart and Grout (2001) provided a scientific basis for poka-yoke (mistake-proofing) concerning human error by drawing upon research from psychology and cognitive science.

Poka-yoke can be very useful in designing and improving service delivery processes when used together with service blueprinting. Originally developed by G. Lynn Shostack (1984, 1992), service blueprinting is a visual representation of a service process as a flow chart (Seyring et al., 2009). It shows how the components of a service are connected and how they interact. Studying the blueprint can help

identify where in the process failures may occur and change the design or develop countermeasures to prevent them. Obviously, service blueprinting can also be used for simply improving the service process and introducing innovations (Kingman-Brundage, 1989; George and Gibson, 1991; Bitner et al., 2008). Clearly, poka-yoke and blueprinting together will improve the resilience and robustness of services and reduce vulnerability to service failure risks.

There are quite a few applications of poka-yoke in numerous services. Lee et al. (2019) provide a taxonomy of security management approaches from the organizational security management perspective for the application of mistake-proofing tools in security management. Jin et al. (2012) proposed a method for the analysis of medication incidents and the systematic planning of error-proofing (EP) countermeasures. Using a panel of healthcare professionals, Kovach et al. (2013) reviewed 150 error-proofing strategies for medical error prevention and ranked them based on effectiveness, cost, ease of implementation, and mitigation of errors. Grout (2006) discussed how healthcare processes should be designed to prevent medical mistakes and improve patient safety. The World Health Organization (WHO, 2016) has published a monograph to raise awareness among WHO member states to reduce medication errors in primary care. This publication covers causes of medication errors and potential solutions.

6.2. Failure Mode and Effect Analysis (FMEA)

Another tool from manufacturing engineering for risk management and risk reduction is FMEA. It was developed for the U.S. military in the 1940s. Its purpose is to identify potential failures or risks in a product or process design, so that they can be eliminated or countermeasures can be implemented. Failure mode means the specific way a product or process can fail. Effect analysis focuses on studying the consequences of those failures.

Application of FMEA requires a multidisciplinary, cross-functional team from all fields of expertise related to the product or process (see https://asq.org/quality-resources/fmea for a step-by-step implementation of FMEA). Most applications of FMEA use root-cause analysis (RCA) and the "5 Why's" process. In a service setting, a successful application of FMEA would reduce the vulnerability of a service process and increase the resilience and robustness of the process.

FMEA can also be used to study product or service failures after they occur, for improvements and developing countermeasures for their prevention. RCA can be used to discover the causes of failures rather than symptoms. RCA is a systematic investigative procedure for identifying the true sources that lead to failures in services and service processes (See NCPS, 2021 for a detailed guideline for RCA). RCA is usually accompanied by the "5 Whys" process (Serrat, 2017; Vidyasagar, 2016). Three other tools from manufacturing, Pareto charts, service blueprinting (or flow charts), and Ishikawa (or Fishbone, or cause-and-effect) diagrams, can be used to aid the FMEA and RCA procedures. These simple, easy-to-use graphical tools are covered in most operations management textbooks.

6.3. Root-Cause-Analysis (RCA)

RCA has widespread applications in risk identification in healthcare. In their seminal report on medical errors, the Institute of Medicine's Committee on Quality of Health Care in America (Kohn et al., 2000) states that RCA "requires that an organization experiencing a sentinel event conduct a root cause analysis, a process for identifying the basic or causal factors of the event." Askari et al. (2017) used FMEA together with RCA to examine the hazards associated with the process of service delivery in the intensive care unit (ICU) of a tertiary hospital in Iran. Chia et al. (2024) studied the integration of Healthcare Failure Mode and Effect Analysis (HFMEA) with RCA and a service blueprint to mitigate medical risks and enhance mass casualty triage efficiency in emergency units. Khorsandi et al. (2012) reviewed the quality of the adverse incident reporting system and the RCA of serious adverse incidents at the Department of Surgery of Ninewells Hospital, in Dundee, United Kingdom. Doggett (2005) reviewed the cause-and-effect diagram, interrelationship diagram, and current reality tree as tools that can be used with RCA.

6.4. Pareto Charts

Named after the Italian economist Vilfredo Pareto, Pareto charts are used to identify the frequency or costs of types of failures in a failed service process so that corrective actions can be focused on the most frequently occurring or most expensive failures first. It is based on the 80/20 rule, which states that 80 percent of failures are caused by 20 percent of possible causes. The cause-and-effect diagram was created by the Japanese quality expert Kaoru Ishikawa (1985, 1991). The diagram is used to identify causes or sources of errors such as equipment, people, materials, environment, and processes. Sub-causes emanating from these are also represented in the diagram.

FMEA and the associated tools have been used in manufacturing and many services (Reid, 2005; McCain, 2006). A detailed coverage of the method can be found in Stamatis (2019). Malekjahan et al. (2025) used FMEA to determine and score existing risks in aviation. Pourmadadkar et al. (2020) conducted a risk assessment study on the CABG (coronary artery bypass grafting) process.

An integrated approach, based on FMEA, Quality Function Deployment (QFD), and MCDM (multiple-criteria decision-making) techniques, is proposed to identify and prioritize the disruptions in the process and present corrective activities to avoid them. Ye et al. (2024) studied steps from COVID-19 patients' admission to intensive care unit to treatment to discharge and found that potential risks existed to cause nosocomial infection. They used a flow chart for process analysis and developed improvement suggestions based on the FMEA. Sun et al. (2025) investigated the effect of healthcare failure mode and effects analysis (HFMEA) in the management of patients with intrathecal morphine pump implantation.

Kuwaiti (2016) conducted a study to analyze the effect of the Six Sigma methodology, together with FMEA, a Pareto chart, and poka-yoke, in reducing medication errors in the outpatient pharmacy in a Saudi Arabia hospital. Hambleton (2005) used FMEA and RCA in examining real or potential failures in a healthcare compliance program.

7. Risks in Air Travel and Their Management

As an example, regarding risks and their management in services, this section will focus on risks in air travel. Air travel is one of the most important industries in the service sector. The following statistics give an idea about the magnitude of airline operations in the U.S.: based on 490 air carriers, a total of 95.3 million departures were performed from January 2014 to June 2024; in 2024 this number was 10,672,803 departures. Between 2002 and 2024, a total of 19,296,544,405 passengers were carried by all airlines; in 2024, the number of passengers of all airlines was 1,107,987,703 (BTS, 2025). IATA (2025) forecasts total passenger revenue for world airlines as $693 billion in 2025.

"Air travel" is used as an umbrella term for its most important components: airlines/airplanes, air traffic control, and airports. Each one of these components has a long list of risks concerning human lives and property. It is not possible or necessary to give an exhaustive list of all these risks to understand the threats to which humans may be exposed; only the most important risks will be reviewed.

The most important risks in airline operations are:

1) Pilot fatigue/pilot health
2) Terrorist attacks targeting airplanes
3) Air traffic control errors
4) Cyber-attacks on airports
5) Runway incursions
6) Runway excursions
7) Unmanned aerial vehicles (UAVs)

Physical and mental pilot fatigue, as well as pilot health, is one of the greatest concerns for airflight safety. Risk literature, as well as healthcare, transportation, and safety literatures, are replete with research and countermeasures on this topic. A Position Paper prepared by a special subcommittee of the Aerospace Human Factors Committee of the Aerospace Medical Association reviewed the relevant scientific literature, summarized applicable U.S. civilian and military flight regulations, evaluated various in-flight and pre-/postflight fatigue countermeasures, and described emerging technologies for detecting and countering fatigue (Caldwell et al., 2009). Hartzler (2014) provided a literature survey detailing both the health and safety concerns of fatigue among commercial pilots, as well as benefits and risks associated with strategic napping to alleviate this fatigue. van Drongelen et al. (2017) surveyed 504 airline pilots through an online questionnaire, including person, work, health, sleep, and lifestyle-related characteristics, to determine risk factors for fatigue among airline pilots.

Wingelaar-Jagt et al. (2021) described the pathophysiology, epidemiology, and effects of fatigue and its impact on aviation, as well as several aspects of fatigue management and recommendations for future research in this field. Minoretti and Emanuele (2023) provided a comprehensive review of the most common health issues experienced by commercial airline pilots and concluded that taking care of pilots' health and ensuring public safety will require a collaborative effort among airlines, governments, and regulators. Zhu and Chen (2023) studied the impact of fatigue on flight safety through a structural equation model and concluded that, compared to physical fatigue, mental fatigue is more likely to occur in pilots and present a more serious risk.

Nicolas (2024) developed a chronological account of major aviation-related terrorist attacks, including the hijacking of aircraft and attacks, and emphasizes the need for advanced technologies and stringent national and international regulations to combat aviation terrorism. Airline hijackings and deaths resulting from them have significantly decreased since the peaks in the 1970s, mainly due to stricter controls and countermeasures taken by governments and airlines (Korecki and Hoika, 2022). Consequently, terrorist attacks on airplanes are still serious but low-probability risks.

Air traffic control errors may originate from the fatigue of controllers or lack of appropriate training. Russeng et al. (2021) found no significant relationship between working period and work fatigue, while work shift and workload have a significant relationship with work fatigue in air traffic controllers. Li et al. (2021) investigated the relationship between traffic volume, air traffic management occurrences, and fatigue with the participation of 57 European Air Navigation Services air traffic controllers (ATCO). They concluded that ATCO fatigue levels are not the main contributory factor associated with air traffic management occurrences. They recommended sufficient rest breaks and roster schedule optimization, as well as task loads that may induce fatigue. Choi (2024) studied risks air traffic controllers may create that cause airline pilots to commit errors during descent and identified understanding controller accents, changes of runway, and difficult clearance of altitude change.

Cyber-attacks are one of the most serious risks. Air traffic control operations, communications, and airport services (check-ins, baggage handling operations) can be disrupted, causing flight cancellations and many hours of flight delays. Cano et al. (2016) analyzed the impact of cyber-attacks whose main goal is to take hold of airport information technology and operations. Gopalakrishnan et al. (2013) recommended a defense-in-depth approach in securing airports from cyber vulnerabilities, where one does not rely on any one security mechanism to prevent all potential threats.

Runway incursions are defined as "Any occurrence at an aerodrome involving the incorrect presence of an aircraft, vehicle, or person on the protected area of a surface designated for the landing and takeoff of aircraft." (FAA, 2025a). Omosebi et al. (2023) investigated the relationship between airport geometry, mitigating

technologies, and the number of runway incursions at 30 large hub airports in the United States using a random effects Poisson model for analyses of panel data. Wang et al. (2018) investigated the factors that contribute to runway incursions.

Another runway risk is runway excursion (RE). "A runway excursion is a veer off or overrun from the runway surface. These surface events occur while an aircraft is taking off or landing and involve many factors ranging from unstable approaches to the condition of the runway" (FAA, 2025b). Lee (2023) investigated the most important causal factors of RE and proposed countermeasures to mitigate potential risks in Taiwan region.

Pyrgies (2019) studied unmanned aerial vehicle (UAV) or drone incidents around airports worldwide and found that "those incidents are more numerous than anticipated and happen higher and further from the airports than expected." Kobaszyńska-Twardowska et al. (2022) proposed a risk management model for dealing with threats to aviation by UAVs. Lykou et al. (2020) presented a survey of drone incidents near airports and a literature review of sensor technologies able to prevent, detect, identify, and mitigate rogue drones. Habler et al. (2023) provide a review of aircraft systems and their various networks, emphasizing the cyber threats to which they are exposed and the impact of a cyber-attack on them and their networks.

Clearly, there are more risks that managers in three components of air travel must deal with, such as supply chain risks (e.g., parts, fuel, and food for airplanes), wildlife strikes, apron accidents, weather events (e.g., snow, hail, thunderstorms, lightning strikes, hurricanes, tornadoes, etc.), and disruptive passengers.

8. Risks in the Hotel and Resort Industry and Their Management

Hotels and resorts constitute another major industry in the service sector. Globally, their market size was estimated to be $1.5 trillion in 2023 (Bachman, 2025). The industry consists of a wide variety of establishments—from small independent hotels to luxury hotels and resorts. Their main functions include the provision of lodging, food services, information, recreation, and entertainment.

The most important risks in the hotel and resort industry are:

1) Natural disaster risk
2) Terrorist attacks
3) Physical/security risk/Theft of valuables
4) Operational risks

8.1. Natural Disaster Risk

Natural disasters like hurricanes, tornadoes, tsunamis, earthquakes put lives of customers and staff and property in risk especially at coastal areas. Managers of these establishments have the duty of reducing the vulnerabilities such as power systems, telecommunications, water, and food supplies. Managers must make sure their systems' vulnerabilities have been reduced. This can be achieved by increas-

ing resilience and robustness of their systems like stocking emergency supplies of food and beverages, constantly monitoring weather reports, having redundant power generation equipment, and maintaining healthcare support (e.g. doctors, nurses, medical emergency responders), arranging alternative lodging for guests and training staff for disaster response. Naturally, these will increase operating costs of a hospitality establishment, however staying vulnerable against natural disaster may have much higher costs in human lives and property damage.

Brown et al. (2019) investigated the measure of disaster resilience within the hotel sector in an exploratory quantitative study. Data were collected from hotel general managers and staff in two New Zealand tourist destinations. They found that hotels in the sample have positive attributes of disaster resilience. They also recommended areas of future focus for resilience-building. Brown et al. (2021) explored hotel disaster resilience with a multiple methods approach, utilizing a capital-based framework. They recommended the need to develop an all-hazards approach to training and exercises and to integrate staff fully in the process. They also stated that the development of multiple resources prior to a disaster and continued investment afterward can enhance and build disaster resilience over time.

Johnston et al. (2007) evaluated staff training for emergencies, emergency management exercises, and hazard signage within motels and hotels in Ocean Shores, Washington, USA. They also made suggestions on how to improve preparedness, including a natural hazard warning system, and training designed within the wider context of effective warning systems: early warning and notification, response planning, discussion and communication, and education. Orchiston (2013) examined tourism business disaster planning in areas at risk from low-frequency/high-consequence natural disasters. The author presented empirical findings from a tourism business survey in the Southern Alps of New Zealand, an area with high seismic risk that supports a tourism industry comprising many micro-sized, owner-operated businesses.

8.2. Terrorist Attacks

Terrorism has been a difficult word to define; there is no legal or scientific agreement on the definition of terrorism. Encyclopedia Britannica (EB, 2025) defines terrorism as the calculated use of violence to create a general climate of fear in a population and thereby to bring about a particular political objective. The FBI's (2025) definition is "Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations." According to a Heritage Foundation Report (Muhlhausen and McNeill, 2011), "Between 1969 and 2009, there were 38,345 terrorist incidents around the world. Of these attacks, 7.8 percent (2981) were directed against the United States." Wernick and Von Glinow (2012) identify the reasons why terrorists target luxury hotels: 1) they are symbolic targets of Western affluence; 2) like restaurants and nightclubs, they are "soft targets"; 3) a successful attack on a five-star property can yield high rewards equivalent to an attack on an embassy; 4)

changing organizational composition of the terrorist groups themselves.

Paraskevas (2013) proposed a six-step baseline strategy to address terrorist threats targeting hotels. Based on the generic crisis management literature, the study showed that there is a need to expand the understanding of the security function from its classic approach of "detect-deny-respond" to a model with six building blocks that can become the framework for the development of a strategy to protect hotels against terrorism.

Department of Homeland Security (DHS, 2010) has prepared a guide to protect the US lodging industry against terrorist attacks and cyber-attacks. The guide outlines the key vulnerabilities of hotels. It discusses manmade hazards, accidents, and natural disasters, and proposes protective measures including planning and preparedness, incident response, monitoring, surveillance, inspection, and information security and cybersecurity to reduce vulnerabilities and increase resilience and robustness. Another useful source for terrorism preparedness and prevention is a handbook edited by Schmid (2021), which contains papers on prevention of preparatory acts, prevention of, and preparedness for, terrorist attacks.

8.3. Physical/Security Risk/Theft of Valuables

Although rare, hotel and resort guests may be targets of physical attacks or their valuables may be stolen. Large hotels usually have security staff and closed-circuit television (CCTV) monitoring hallways of guest rooms and other critical parts of the hotel (e.g., garage, delivery areas), as well as well-designed lighting of hallways and corridors. Training for both the security and general staff and installing a state-of-the-art CCTV system would reduce the vulnerability of guests and their property.

8.4. Operational Risks

Hotels have many departments and systems to serve their guests. Some of these include front office, booking and reservation, restaurant(s), bar(s), kitchen, food and beverage, room service, housekeeping, laundry, heating and cooling, plumbing, electrical, telecommunications, maintenance, and event and conference management. Another particularly important operational risk is the supply risk. Hotels have a complex supply chain and a variety of suppliers like food, beverage, linen, toiletries, cleaning, and maintenance supplies. Establishing strong ties and partnerships with suppliers for timely delivery of supplies and maintaining optimal inventory levels goes a long way to reduce most of the operational risks. Smooth operation of these systems is essential for guest satisfaction and hotel profits. Like any system, failures may happen in one or more of them; consequently, constantly monitoring and updating these systems and staff training are critical duties of hotel management.

9. Summary and Conclusion

This paper presented a review of risks in organizations and specific risks in ser-

vices. Risk definitions from the risk research area, together with frameworks proposed by risk professional societies, specifically risk management (RM) and enterprise risk management (ERM), have been reviewed. In addition, concepts of vulnerability, resilience, and robustness, and the important roles they play in risk management, were discussed. Tools and methods, mostly from manufacturing management, were proposed as potential aids in reducing vulnerability and increasing resilience and robustness of organizations in their struggle with various risks. Finally, risks and their management in air travel (i.e., airlines, air traffic control, and airports) and hotel and resort industries were discussed as two examples.

This paper is an attempt to contribute to the literature in a long-neglected area of services research, namely risks in services in general and their management. This paper also reviews and recommends the application of tools and methods to reduce the vulnerability of service organizations and improve their resilience and robustness in dealing with a variety of risks, thereby equipping service managers for the defense of their organizations.

As mentioned above, the literature survey revealed only one journal publication on risks in services in general and their management. Being the second journal article on the subject, this paper may revive interest among service researchers to focus on this long-neglected area of service management. It is hoped that this paper will alert researchers to a wide-open area of services research and will encourage them to investigate various aspects of risks in services.

Future research may focus on risks in other service industries, such as specific healthcare branches, in more detail. Also, some researchers may investigate the applications of management science/operations research techniques for optimizing the resilience and robustness of service systems.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

Adger, W. N. (2006). Vulnerability. *Global Environmental Change, 16,* 268-281. https://doi.org/10.1016/j.gloenvcha.2006.02.006

Althaus, C. E. (2005). A Disciplinary Perspective on the Epistemological Status of Risk. *Risk Analysis, 25,* 567-588. https://doi.org/10.1111/j.1539-6924.2005.00625.x

Anton, S. G., & Nucu, A. E. A. (2020). Enterprise Risk Management: A Literature Review and Agenda for Future Research. *Journal of Risk and Financial Management, 13,* Article 281. https://doi.org/10.3390/jrfm13110281

Askari, R., Shafii, M., Rafiei, S., Abolhassani, M. S., & Salarikhah, E. (2017). Failure Mode and Effect Analysis: Improving Intensive Care Unit Risk Management Processes. *International Journal of Health Care Quality Assurance, 30,* 208-215. https://doi.org/10.1108/ijhcqa-04-2016-0053

Aven, T. (2011). On Some Recent Definitions and Analysis Frameworks for Risk, Vulnerability, and Resilience. *Risk Analysis, 31,* 515-522. https://doi.org/10.1111/j.1539-6924.2010.01528.x

Aven, T., & Renn, O. (2009). On Risk Defined as an Event Where the Outcome Is Uncertain. *Journal of Risk Research, 12,* 1-11. https://doi.org/10.1080/13669870802488883

Aven, T., Ben-Haim, Y., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., Kröger, W., Renn, O., Thompson, K. M., & Zio, E. (2018). *Society for Risk Analysis Glossary.* https://www.sra.org/risk-analysis-introduction/risk-analysis-glossary/

Bachman, W. (2025). *How the Travel & Hospitality Industry Works.* Umbrex.

Barasa, E., Mbau, R., & Gilson, L. (2018). What Is Resilience and How Can It Be Nurtured? A Systematic Review of Empirical Literature on Organizational Resilience. *International Journal of Health Policy and Management, 7,* 491-503. https://doi.org/10.15171/ijhpm.2018.06

Berkes, F. (2007). Understanding Uncertainty and Reducing Vulnerability: Lessons from Resilience Thinking. *Natural Hazards, 41,* 283-295. https://doi.org/10.1007/s11069-006-9036-7

Bitner, M. J., Ostrom, A. L., & Morgan, F. N. (2008). Service Blueprinting: A Practical Technique for Service Innovation. *California Management Review, 50,* 66-94. https://doi.org/10.2307/41166446

Bongiovanni, I., & Newton, C. (2019). Toward an Epidemiology of Safety and Security Risks: An Organizational Vulnerability Assessment in International Airports. *Risk Analysis, 39,* 1281-1297. https://doi.org/10.1111/risa.13238

Brand, F. S., & Jax, K. (2007). Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Object. *Ecology and Society, 12,* Article 23. https://doi.org/10.5751/es-02029-120123

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning, 48,* 265-276. https://doi.org/10.1016/j.lrp.2014.07.005

Brown, N. A., Feldmann-Jensen, S., Rovins, J. E., Orchiston, C., & Johnston, D. (2021). Exploring Disaster Resilience within the Hotel Sector: A Case Study of Wellington and Hawke's Bay New Zealand. *International Journal of Disaster Risk Reduction, 55,* Article ID: 102080. https://doi.org/10.1016/j.ijdrr.2021.102080

Brown, N. A., Rovins, J. E., Feldmann-Jensen, S., Orchiston, C., & Johnston, D. (2019). Measuring Disaster Resilience within the Hotel Sector: An Exploratory Survey of Wellington and Hawke's Bay, New Zealand Hotel Staff and Managers. *International Journal of Disaster Risk Reduction, 33,* 108-121. https://doi.org/10.1016/j.ijdrr.2018.09.014

BTS (2025). *Bureau of Transportation Statistics, U.S. Department of Transportation.* https://www.transtats.bts.gov/Data_Elements.aspx?Data=4

Caldwell, J. A., Mallis, M. M., Caldwell, J. L., Paul, M. A., Miller, J. C., & Neri, D. F. (2009). Fatigue Countermeasures in Aviation. *Aviation, Space, and Environmental Medicine, 80,* 29-59. https://doi.org/10.3357/asem.2435.2009

Campbell, S. (2005). Determining Overall Risk. *Journal of Risk Research, 8,* 569-581. https://doi.org/10.1080/13669870500118329

Cano, J., Pollini, A., Falciani, L., & Turhan, U. (2016). Modeling Current and Emerging Threats in the Airport Domain through Adversarial Risk Analysis. *Journal of Risk Research, 19,* 894-912. https://doi.org/10.1080/13669877.2015.1057201

CAS (Casualty Actuarial Society) (2003). *Overview of Enterprise Risk Management.* https://www.casact.org/sites/default/files/database/forum_03sforum_03sf099.pdf

CD (Cambridge Dictionary) (2025). *Vulnerability.* https://dictionary.cambridge.org/dictionary/english/vulnerability

Chase, R. B., & Stewart, D. M. (1995). *Mistake-Proofing: Designing Errors Out.* Productiv-

ity Press.

Chase, R., & Stewart, D. (1994). Make Your Service Fail-Safe. *Sloan Management Review, 35,* 35-44.

Chia, J., Chang, C., Lo, S., Yang, C., & Yang, H. (2024). Healthcare Failure Mode and Effect Analysis Combined Service Blueprint—Mitigating Mass Casualty Triage in Emergency Units: A Qualitative Study. *International Emergency Nursing, 77,* Article ID: 101508. https://doi.org/10.1016/j.ienj.2024.101508

Choi, J. (2024). Air Traffic Control Threats to Pilots through Line Operations Safety Audits. *The Korean Journal of Aerospace and Environmental Medicine, 34,* 19-22. https://doi.org/10.46246/kjasem.240005

Christopher, M., & Peck, H. (2004). Building the Resilient Supply Chain. *The International Journal of Logistics Management, 15,* 1-14. https://doi.org/10.1108/09574090410700275

COSO (2017). *Enterprise Risk Management: Integrating with Strategy and Performance, Executive Summary.*

COSO (Committee of Sponsoring Organizations of the Treadway Commission) (2020). Compliance Risk Management: Applying the COSO ERM Framework.

Crouhy, M., Galai, D., & Mark, R. (2023). *The Essentials of Risk Management* (3rd ed.). McGraw-Hill.

Damali, U., Secchi, E., Tax, S. S., & McCutcheon, D. (2021). Customer Participation Risk Management: Conceptual Model and Managerial Assessment Tool. *Journal of Service Management, 32,* 27-51. https://doi.org/10.1108/josm-05-2018-0147

DHS (2010). *Protective Measures Guide for the U.S. Lodging Industry.* Department of Homeland Security.

Dillon, R. D., Feldhaus, W. R., & Farrell, R. P. (1984). A Special Area of Service: Risk Management. *Journal of Accountancy,* 50-58.

DoD News Briefing (2002). *Secretary Rumsfeld and Gen. Myers, Presenter: Secretary of Defense Donald H. Rumsfeld, February 12, 11:30 a.m. EDT.*

Doggett, A. M. (2005). Root Cause Analysis: A Framework for Tool Selection. *Quality Management Journal, 12,* 34-45. https://doi.org/10.1080/10686967.2005.11919269

Dvorak, P. (1998). Poka-Yoke Designs Make Assemblies Mistake Proof. *Machine Design, 70,* 181-184.

EB (Encyclopedia Britannica) (2025). *Terrorism.* https://www.britannica.com/topic/terrorism

FAA (Federal Aviation Administration) (2025a). *Runway Incursions.* https://www.faa.gov/airports/runway_safety/resources/runway_incursions

FAA (Federal Aviation Administration) (2025b). *Runway Excursions.* https://www.faa.gov/airports/runway_safety/excursion

FBI (Federal Bureau of Investigation) (2025). https://www.fbi.gov/investigate/terrorism

Fleming, R. S. (1998). Assessing Organizational Vulnerability to Acts of Terrorism. *Advanced Management Journal, 63,* 27-32.

Francis, G. (2019). Enterprise Risk Management (ERM): Key Risks, Responses and Applications. In *Enterprise Risk Management Symposium* (pp. 1-22). Canadian Institute of Actuaries, Casualty Actuarial Society, and Society of Actuaries.

Fraser, J. R. S., Quail, R., & Simkins, B. J. (2021). *Enterprise Risk Management* (2nd ed.). Wiley.

Fraser, J., Quail, R., & Simkins, B. (2024). What's Wrong with Enterprise Risk Manage-

ment? *Journal of Risk and Financial Management, 17,* Article 274. https://doi.org/10.3390/jrfm17070274

Gallopín, G. C. (2006). Linkages between Vulnerability, Resilience, and Adaptive Capacity. *Global Environmental Change, 16,* 293-303. https://doi.org/10.1016/j.gloenvcha.2006.02.004

Gardoni, P., & Murphy, C. (2014). A Scale of Risk. *Risk Analysis, 34,* 1208-1227. https://doi.org/10.1111/risa.12150

George, W. R., & Gibson, B. E. (1991). Blueprinting: A Tool for Managing Quality in Service. In S. W. Brown, E. Gummesson, B. Edvardsson, & B. O. Gustavsson (Eds.), *Service Quality* (pp. 73-91). Lexington Books.

Gheorghe, A. V., & Vamanu, D. V. (2004). Towards QVA—Quantitative Vulnerability Assessment: A Generic Practical Model. *Journal of Risk Research, 7,* 613-628. https://doi.org/10.1080/1366987042000192219

Gopalakrishnan, K., Govindarasu, M., W. Jacobson, D., & M. Phares, B. (2013). Cyber Security for Airports. *International Journal for Traffic and Transport Engineering, 3,* 365-376. https://doi.org/10.7708/ijtte.2013.3(4).02

Grout, J. R. (2006). Mistake Proofing: Changing Designs to Reduce Error. *Quality in Health Care, 15,* i44-i49. https://doi.org/10.1136/qshc.2005.016030

Habler, E., Bitton, R., & Shabtai, A. (2023). Assessing Aircraft Security: A Comprehensive Survey and Methodology for Evaluation. *ACM Computing Surveys, 56,* 1-40. https://doi.org/10.1145/3610772

Haimes, Y. Y. (2009). On the Definition of Resilience in Systems. *Risk Analysis, 29,* 498-501. https://doi.org/10.1111/j.1539-6924.2009.01216.x

Halekotte, L., Mentges, A., & Lichte, D. (2025). Do We Practice What We Preach? The Dissonance between Resilience Understanding and Measurement. *International Journal of Disaster Risk Reduction, 118,* Article ID: 105265. https://doi.org/10.1016/j.ijdrr.2025.105265

Hall, C. M., Safonov, A., & Naderi Koupaei, S. (2023). Resilience in Hospitality and Tourism: Issues, Synthesis and Agenda. *International Journal of Contemporary Hospitality Management, 35,* 347-368. https://doi.org/10.1108/ijchm-11-2021-1428

Hambleton, M. (2005). Applying Root Cause Analysis and Failure Mode and Effect Analysis to Our Compliance Programs. *Journal of Healthcare Compliance, 7,* 5-12.

Hardy, K. (2015). *Enterprise Risk Management: A Guide for Government Professionals.* Jossey-Bass.

Hartzler, B. M. (2014). Fatigue on the Flight Deck: The Consequences of Sleep Loss and the Benefits of Napping. *Accident Analysis & Prevention, 62,* 309-318. https://doi.org/10.1016/j.aap.2013.10.010

Hayes, A. (2025). *Enterprise Risk Management (ERM): What It Is and How It Works.* https://www.investopedia.com/terms/e/enterprise-risk-management.asp

Hollings, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics, 4,* 1-23. https://doi.org/10.1146/annurev.es.04.110173.000245

Hollman, K. W., & Forrest, J. E. (1991). Risk Management in a Service Business. *International Journal of Service Industry Management, 2,* 49-65. https://doi.org/10.1108/09564239110144993

Hollman, K. W., & Mohammad-Zadek, S. (1984). Risk Management in Small Businesses. *Journal of Small Business Management, 22,* 47-55.

Horvey, S. S., & Odei-Mensah, J. (2023). The Measurements and Performance of Enterprise Risk Management: A Comprehensive Literature Review. *Journal of Risk Research, 26,*

778-800. https://doi.org/10.1080/13669877.2023.2208138

IATA (2025). *Industry Statistics.* https://www.iata.org/en/iata-repository/pressroom/fact-sheets/industry-statistics/

Ishikawa, K. (1985). *What Is Total Quality Control? The Japanese Way.* Prentice Hall Direct.

Ishikawa, K. (1991). *Guide to Quality Control.* Asian Productivity Organization.

ISO (2018). *ISO 31000:2018(en) Risk management—Guidelines.* https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en

Jin, H., Munechika, M., Sano, M., & Kajihara, C. (2012). Four Steps to Reduce Medical Incidents. *International Journal of Quality and Service Sciences, 4,* 399-407. https://doi.org/10.1108/17566691211288377

Johnson, J. E., & Flanigan, G. B. (1977). Exceptions to Current Risk Dichotomies. *The Journal of Risk and Insurance, 44,* 329-334. https://doi.org/10.2307/252146

Johnston, D., Becker, J., Gregg, C., Houghton, B., Paton, D., Leonard, G. et al. (2007). Developing Warning and Disaster Response Capacity in the Tourism Sector in Coastal Washington, Usa. *Disaster Prevention and Management: An International Journal, 16,* 210-216. https://doi.org/10.1108/09653560710739531

Kamalipoor, M., Akbari, M., Nazarian, A., & Hejazi, S. R. (2023). Vulnerability Reduction of Technology-Based Business Research in the Last Four Decades: A Bibliometric Analysis. *Iranian Journal of Management Studies, 16,* 97-123.

Kaplan, R. S., & Mikes, A. (2012). Managing Risks: A New Framework. *Harvard Business Review, 90,* 48-60.

Kaplan, S., & Garrick, B. J. (1981). On the Quantitative Definition of Risk. *Risk Analysis, 1,* 11-27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Khorsandi, M., Skouras, C., Beatson, K., & Alijani, A. (2012). Quality Review of an Adverse Incident Reporting System and Root Cause Analysis of Serious Adverse Surgical Incidents in a Teaching Hospital of Scotland. *Patient Safety in Surgery, 6,* Article No. 21. https://doi.org/10.1186/1754-9493-6-21

Kim, S. D. (2017). Characterization of Unknown Unknowns Using Separation Principles in Case Study on Deepwater Horizon Oil Spill. *Journal of Risk Research, 20,* 151-168. https://doi.org/10.1080/13669877.2014.983949

Kingman-Brundage, J. (1989). The ABCs of Service System Blueprinting: Designing a Winning Service Strategy. In M. Bitner, & L. Crosby (Eds.), *Designing a Winning Service Strategy* (pp. 30-33). American Marketing Association.

Kobaszyńska-Twardowska, A., Łukasiewicz, J., & Sielicki, P. W. (2022). Risk Management Model for Unmanned Aerial Vehicles during Flight Operations. *Materials, 15,* Article 2448. https://doi.org/10.3390/ma15072448

Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (2000). *To Err Is Human: Building a Safer Health System.* Committee on Quality of Health Care in America; Institute of Medicine, The National Academies Press. https://doi.org/10.17226/9728

Korecki, Z., & Hoika, T. (2022). Effectiveness of Preventive Security Measures and Criminal Acts against Civil Aviation. *Transport Problems, 17,* 107-114. https://doi.org/10.20858/tp.2022.17.2.09

Kovach, J. V., Revere, L., & Black, K. (2013). Error Proofing Healthcare: An Analysis of Low Cost, Easy to Implement and Effective Solutions. *Leadership in Health Services, 26,* 107-117. https://doi.org/10.1108/17511871311319704

Kruk, M. E., Myers, M., Varpilah, S. T., & Dahn, B. T. (2015). What Is a Resilient Health

System? Lessons from Ebola. *The Lancet, 385,* 1910-1912. https://doi.org/10.1016/s0140-6736(15)60755-3

Kubacki, K., Siemieniako, D., & Brennan, L. (2020). Building Positive Resilience through Vulnerability Analysis. *Journal of Social Marketing, 10,* 471-488. https://doi.org/10.1108/jsocm-09-2019-0142

Kuwaiti, A. A. (2016). Application of Six Sigma Methodology to Reduce Medication Errors in the Outpatient Pharmacy Unit: A Case Study from King Fahd University Hospital, Saudi Arabia. *International Journal for Quality Research, 10,* 267-278.

Lee, H., Han, C., & Yoo, T. (2019). The Application of Mistake-Proofing to Organisational Security Management. *Total Quality Management & Business Excellence, 30,* 1151-1166. https://doi.org/10.1080/14783363.2017.1360133

Lee, Y. (2023). Causal Factors Analysis of Runway Excursion Occurrences through Fuzzy Logic Modeling Method. *Transportation Engineering, 14,* Article ID: 100204. https://doi.org/10.1016/j.treng.2023.100204

Leino, H. M., Davey, J., & Johns, R. (2024). Service System Resilience under Resource Scarcity: From Vulnerability to Balanced Centricity. *Journal of Services Marketing, 38,* 113-130. https://doi.org/10.1108/jsm-01-2023-0024

Levin, S. A., & Lubchenco, J. (2008). Resilience, Robustness, and Marine Ecosystem-Based Management. *BioScience, 58,* 27-32. https://doi.org/10.1641/b580107

Li, W., Kearney, P., Zhang, J., Hsu, Y., & Braithwaite, G. (2021). The Analysis of Occurrences Associated with Air Traffic Volume and Air Traffic Controllers' Alertness for Fatigue Risk Management. *Risk Analysis, 41,* 1004-1018. https://doi.org/10.1111/risa.13594

Lykou, G., Moustakas, D., & Gritzalis, D. (2020). Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. *Sensors, 20,* Article 3537. https://doi.org/10.3390/s20123537

Malekjahan, A. N., Husseinzadeh Kashan, A., & Sajadi, S. M. (2025). A Novel Sequential Risk Assessment Model for Analyzing Commercial Aviation Accidents: Soft Computing Perspective. *Risk Analysis, 45,* 128-153. https://doi.org/10.1111/risa.14486

McCain, C. (2006). Using an FMEA in a Service Setting. *Quality Progress, 39,* 24-29.

McEntire, D. (2011). Understanding and Reducing Vulnerability: From the Approach of Liabilities and Capabilities. *Disaster Prevention and Management: An International Journal, 20,* 294-313. https://doi.org/10.1108/09653561111141736

Melnyk, S. A., Closs, D. J., Griffis, S. E., Zobel, C. W., & Macdonald, J. R. (2014). Understanding Supply Chain Resilience. *Supply Chain Management Review, 18,* 34-41.

Mentges, A., Halekotte, L., Schneider, M., Demmer, T., & Lichte, D. (2023). A Resilience Glossary Shaped by Context: Reviewing Resilience-Related Terms for Critical Infrastructures. *International Journal of Disaster Risk Reduction, 96,* Article ID: 103893. https://doi.org/10.1016/j.ijdrr.2023.103893

Minoretti, P., & Emanuele, E. (2023). Health in the Skies: A Narrative Review of the Issues Faced by Commercial Airline Pilots. *Cureus, 15,* e38000. https://doi.org/10.7759/cureus.38000

Mishra, B. K., Rolland, E., Satpathy, A., & Moore, M. (2019). A Framework for Enterprise Risk Identification and Management: The Resource-Based View. *Managerial Auditing Journal, 34,* 162-188. https://doi.org/10.1108/maj-12-2017-1751

Muhlhausen, D. B., & McNeill, J. B. (2011). *Terror Trends: 40 Years' Data on International and Domestic Terrorism.* The Heritage Foundation Report. https://www.heritage.org/terrorism/report/terror-trends-40-years-data-international-and-domestic-terrorism

MW (Merriam-Webster) (2025). https://www.merriam-webster.com/dictionary/vulnerability?src=search-dict-box

Nason, R., & Livvarcin, O. (2020). *Risk Management for Nonprofit Organizations.* Business Expert Press.

NCPS (2021). *Guide to Performing a Root Cause Analysis.* VHA National Center for Patient Safety. https://www.patientsafety.va.gov/docs/RCA-Guidebook_02052021.pdf

Neuvel, J. M. M., de Boer, D. J., & Rodenhuis, W. K. F. (2015). Managing Vulnerability: The Implementation of Vulnerability Reduction Measures. *Journal of Risk Research, 18,* 182-198. https://doi.org/10.1080/13669877.2014.889193

Nicolas, R. (2024). Terrorism: The Challenge of Aviation Security. *Agora International Journal of Juridical Sciences, 18,* 225-230. https://doi.org/10.15837/aijjs.v18i1.6758

Nocco, B. W., & Stulz, R. M. (2022). Enterprise Risk Management: Theory and Practice. *Journal of Applied Corporate Finance, 34,* 81-94. https://doi.org/10.1111/jacf.12490

Nordin, F., Kindström, D., Kowalkowski, C., & Rehme, J. (2011). The Risks of Providing Services: Differential Risk Effects of the Service-Development Strategies of Customisation, Bundling, and Range. *Journal of Service Management, 22,* 390-408. https://doi.org/10.1108/09564231111136881

Nyanchama, M. (2005). Enterprise Vulnerability Management and Its Role in Information Security Management. *Information Systems Security, 14,* 29-56. https://doi.org/10.1201/1086.1065898x/45390.14.3.20050701/89149.6

O'Connor, P., Esfandiar, K., & Hallak, R. (2025). Resilience for Hospitality and Tourism Enterprises: A Review and Directions for Future Research. *Tourism Analysis, 30,* 5-22. https://doi.org/10.3727/108354224x17209729214520

Olson, D. G., & Simkiss, J. A. (1982). An Overview of Risk Management. *The Geneva Papers on Risk and Insurance—Issues and Practice, 7,* 114-128. https://doi.org/10.1057/gpp.1982.7

Omosebi, O., Azimi, M., Olowokere, D., Wanyan, Y., Zhao, Q., & Qi, Y. (2023). Investigating Runway Incursion Incidents at United States Airports. *Future Transportation, 3,* 1209-1222. https://doi.org/10.3390/futuretransp3040066

Orchiston, C. (2013). Tourism Business Preparedness, Resilience and Disaster Planning in a Region of High Seismic Risk: The Case of the Southern Alps, New Zealand. *Current Issues in Tourism, 16,* 477-494. https://doi.org/10.1080/13683500.2012.741115

Paape, L., & Speklé, R. F. (2012). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review, 21,* 533-564. https://doi.org/10.1080/09638180.2012.661937

Paraskevas, A. (2013). Aligning Strategy to Threat: A Baseline Anti-Terrorism Strategy for Hotels. *International Journal of Contemporary Hospitality Management, 25,* 140-162. https://doi.org/10.1108/09596111311290264

Paschoalotto, M. A. C., Lazzari, E. A., Rocha, R., Massuda, A., & Castro, M. C. (2023). Health Systems Resilience: Is It Time to Revisit Resilience after Covid-19? *Social Science & Medicine, 320,* Article ID: 115716. https://doi.org/10.1016/j.socscimed.2023.115716

Pinto, A. C., & Magpili, L. (2015). *Operational Risk Management.* Momentum Press.

Pourmadadkar, M., Beheshtinia, M. A., & Ghods, K. (2020). An Integrated Approach for Healthcare Services Risk Assessment and Quality Enhancement. *International Journal of Quality & Reliability Management, 37,* 1183-1208. https://doi.org/10.1108/ijqrm-11-2018-0314

Pyrgies, J. (2019). The Uavs Threat to Airport Security: Risk Analysis and Mitigation. *Journal of Airline and Airport Management, 9,* 63-96. https://doi.org/10.3926/jairm.127

Reid, R. D. (2005). *FEMA-Something Old, Something New* (pp. 90-93). Quality Progress.

Rejda, G. E., McNamara, M. J., & Rabel, W. H. (2022). *Principles of Risk Management and Insurance* (14th ed.). Pearson Education Limited.

RIMS (The Risk Management Society) (2025). *What Is Enterprise Risk Management?* https://www.rims.org/resources/strategic-enterprise-risk-center/about-serm

Rosa, E. A. (1998). Metatheoretical Foundations for Post-Normal Risk. *Journal of Risk Research, 1,* 15-44. https://doi.org/10.1080/136698798377303

Russeng, S. S., Saleh, L. M., Mallongi, A., & Hoy, C. (2021). The Relationship among Working Period, Work Shift, and Workload to Work Fatigue in Air Traffic Controllers at Sultan Hasanuddin Airport. *Gaceta Sanitaria, 35,* S404-S407. https://doi.org/10.1016/j.gaceta.2021.10.062

Schmid, A. P. (2021). *Handbook of Terrorism Prevention and Preparedness.* International Center for Counter-Terrorism.

Schneier, R., & Miccolis, J. (1998). RISK: Enterprise management. *Strategy & Leadership, 26,* 10-16. https://doi.org/10.1108/eb054613

Scholz, R. W., Blumer, Y. B., & Brand, F. S. (2012). Risk, Vulnerability, Robustness, and Resilience from a Decision-Theoretic Perspective. *Journal of Risk Research, 15,* 313-330. https://doi.org/10.1080/13669877.2011.634522

Serrat, O. (2017). The Five Whys Technique. In O. Serrat (Ed.), *Knowledge Solutions* (pp. 307-310). Springer Singapore. https://doi.org/10.1007/978-981-10-0983-9_32

Seyring, M, Dornberger, U., Suvelza, A., & Byrnes, T. (2009). *Service Blueprinting Handbook.* Small Enterprise Promotion + Training, Universität Leipzig.

Shingo, S. (1986). *Zero Quality Control: Source Inspection and the Poka-Yoke System.* Cambridge Productivity Press.

Shostack, L. G. (1984). *Designing Services That Deliver* (pp. 133-139). Harvard Business Review.

Shostack, L. G. (1992). Understanding Services Through Blueprinting. In T. A. Swartz, D. E. Bowen, & S. W. Brown (Eds.), *Advances in Services Marketing and Management: Research and Practice* (pp. 75-90). JAI Press Inc.

Sobel, P. J., & Reding, K. F. (2004). Aligning Corporate Governance with Enterprise Risk Management. *Management Accounting Quarterly, 5,* 29-37.

Stamatis, D. H. (2019). *Risk Management Using Failure Mode and Effect Analysis (FMEA).* American Society for Quality, Quality Press.

Stewart, D. M. (2003). Piecing Together Service Quality: A Framework for Robust Service. *Production and Operations Management, 12,* 246-265. https://doi.org/10.1111/j.1937-5956.2003.tb00503.x

Stewart, D. M., & Grout, J. R. (2001). The Human Side of Mistake-Proofing. *Production and Operations Management, 10,* 440-459. https://doi.org/10.1111/j.1937-5956.2001.tb00086.x

Stewart, D. M., & Melnyk, S. A. (2000). Effective Process Improvement: Developing Poka-Yoke Processes. *Production and Inventory Management Journal, 41,* 48-55.

Sun, L., Fang, M., Xu, T., Liu, M., Fang, S., & Feng, W. (2025). Application of Healthcare Failure Mode and Effect Analysis in the Management of Patients with Intrathecal Morphine Pump Implantation. *Pain Management Nursing, 26,* e207-e214. https://doi.org/10.1016/j.pmn.2024.10.019

Taguchi, G. (1986). *Introduction to Quality Engineering: Designing Quality into Products and Processes.* Quality Resources.

Taguchi, G., & Clausing, D. (1990). *Robust Quality* (pp. 62-75). Harvard Business Review.

Taguchi, G., Chowdhury, S., & Wu, Y. (2005). *Taguchi's Quality Engineering Handbook.* John Wiley and Sons.

Taleb, N. N., Goldstein, D. G., & Spitznagel, M. W. (2009). *The Six Mistakes Executives Make in Risk Management* (pp. 78-81). Harvard Business Review.

Tasic, J., Amir, S., Tan, J., & Khader, M. (2020). A Multilevel Framework to Enhance Organizational Resilience. *Journal of Risk Research, 23,* 713-738. https://doi.org/10.1080/13669877.2019.1617340

Tortorella, G., Prashar, A., Antony, J., Vassolo, R., Mac Cawley, A., Peimbert Garcia, R. et al. (2023). Soft Lean Practices and Organizational Resilience in the Service Sector. *Management Decision, 62,* 1424-1452. https://doi.org/10.1108/md-06-2023-1034

Vainieri, M., Caputo, A., & Vinci, A. (2024). Resilience Dimensions in Health System Performance Assessments, European Union. *Bulletin of the World Health Organization, 102,* 498-508. https://doi.org/10.2471/blt.23.291102

van Drongelen, A., Boot, C. R. L., Hlobil, H., Smid, T., & van der Beek, A. J. (2017). Risk Factors for Fatigue among Airline Pilots. *International Archives of Occupational and Environmental Health, 90,* 39-47. https://doi.org/10.1007/s00420-016-1170-2

Vidyasagar, A. (2016). The Art of Root Cause Analysis. *Quality Progress, 49,* 48.

Walker, B. H. (2020). Resilience: What It Is and Is Not. *Ecology and Society, 25,* Article 11. https://doi.org/10.5751/es-11647-250211

Wandelt, S., Zhang, A., & Sun, X. (2025). Global Airport Resilience Index: Towards a Comprehensive Understanding of Air Transportation Resilience. *Transportation Research Part D: Transport and Environment, 138,* Article ID: 104522. https://doi.org/10.1016/j.trd.2024.104522

Wang, C., Hubbard, S., & Zakharov, W. (2018). Utilizing the Systematic Literature Review in Aviation: A Case Study for Runway Incursions. *Collegiate Aviation Review International, 36,* 34-57. https://doi.org/10.22488/okstate.18.100489

Weiss, E. N., & Goldberg, R. (2019). Robust Services: People or Processes? *Business Horizons, 62,* 521-527. https://doi.org/10.1016/j.bushor.2019.03.006

Wernick, D. A., & Von Glinow, M. A. (2012). Reflections on the Evolving Terrorist Threat to Luxury Hotels: A Case Study on Marriott International. *Thunderbird International Business Review, 54,* 729-746. https://doi.org/10.1002/tie.21496

WHO (World Health Organization) (2016). *Medication Errors: Technical Series on Safer Primary Care.*

Williams, C. A. (1966). Attitudes toward Speculative Risks as an Indicator of Attitudes toward Pure Risks. *The Journal of Risk and Insurance, 33,* 577-586. https://doi.org/10.2307/251231

Wingelaar-Jagt, Y. Q., Wingelaar, T. T., Riedel, W. J., & Ramaekers, J. G. (2021). Fatigue in Aviation: Safety Risks, Preventive Strategies and Pharmacological Interventions. *Frontiers in Physiology, 12,* Article 712628. https://doi.org/10.3389/fphys.2021.712628

Wolke, T. (2017). *Risk Management.* Walter de Gruyter GmbH.

Ye, M., Tang, F., Chien, C., Chuang, Y., Liou, J. J. H., & Qu, X. (2024). Application of Failure Mode and Effect Analysis in ICU Admission of Potentially COVID-19 Infected Patients. *American Journal of Infection Control, 52,* 552-562. https://doi.org/10.1016/j.ajic.2023.12.012

Zheng, C., Li, Z., & (Snow) Wu, J. (2021). Tourism Firms' Vulnerability to Risk: The Role of Organizational Slack in Performance and Failure. *Journal of Travel Research, 61,* 990-

1005. https://doi.org/10.1177/00472875211014956

Zhu, S., & Chen, J. (2023). Influence of Fatigue on Flight Safety: A Structural Equation Modeling Analysis. *Applied Mathematics and Nonlinear Sciences, 8,* 3371-3382. https://doi.org/10.2478/amns.2023.2.01135

Appendix Notes

SIDEBAR: ERM Frameworks by three professional societies:

COSO (2017)

1) Governance and Culture: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

2) Strategy and Objective-Setting: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with the strategy; business objectives put the strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

3) Performance: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

4) Review and Revision: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

5) Information, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

ISO (2018)

1) Communication and Consultation: Assist relevant stakeholders in understanding risk, the basis on which decisions are made, and the reasons why particular actions are required.

2) Scope, Context, and Criteria: Customize the risk management process, enabling effective risk assessment and appropriate risk treatment.

3) Risk Assessment (Risk Identification, Risk Analysis, Risk Evaluation): Conducted systematically, iteratively, and collaboratively, drawing on the knowledge and views of stakeholders.

4) Risk Treatment: Select options for addressing risk. Specify how the chosen treatment options will be implemented.

5) Monitoring and Review: Assure and improve the quality and effectiveness of process design, implementation, and outcomes.

6) Recording and Reporting: The risk management process and its outcomes should be documented and reported through appropriate mechanisms.

SIDEBAR: ERM Frameworks by three professional societies (continued):

CAS (2003)

1) Establish Context: Define the relationship of the enterprise with its external and internal environments. Identify the risk categories relevant to the enterprise.

2) Identify Risks: Document the conditions and events (including "extreme events") that represent material threats to the enterprise's achievement of its objectives or represent areas to exploit for competitive advantage.

3) Analyze/Quantify Risks: Calibrate and, wherever possible, create probability distributions of outcomes for each material risk.

4) Integrate Risks: aggregating all risk distributions, reflecting correlations and portfolio effects, and expressing the results in terms of the impact on the enterprise's key performance indicators (i.e., the "aggregate risk profile").

5) Assess/Prioritize Risks: Determine the contribution of each risk to the aggregate risk profile, and prioritize accordingly, so that decisions can be made regarding the appropriate treatment.

6) Treat/Exploit Risks: Develop strategies, including decisions to avoid, retain (and finance), reduce, transfer, or exploit risk.

7) Monitor & Review: Continually gauge the risk environment and the performance of the risk management strategies.