Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk

Svana Helen Björnsdottir [1,*], Pall Jensson [1], Saemundur E. Thorsteinsson [2], Ioannis M. Dokas [3] and Robert J. de Boer [4]

1   Department of Engineering, Reykjavik University, 101 Reykjavík, Iceland; pallj@ru.is
2   Department of Engineering, University of Iceland, 101 Reykjavík, Iceland; saemi@hi.is
3   Department of Civil Engineering, Democritus University of Thrace, 69100 Komotini, Greece; idokas@civil.duth.gr
4   Department of Engineering, SDO University of Applied Sciences, 3142 GC Maassluis, The Netherlands; robertjan.deboer@xs4all.nl
*   Correspondence: svanahb@ru.is; Tel.: +354-89-99-200

Abstract: The overall aim of this article is to contribute to the further development of the area of benchmarking in risk management. The article introduces a two-step benchmarking model to assess the efficacy of ISO risk management systems. It furthermore aims at verifying its usefulness in terms of finding hidden risk issues and improvement opportunities. The existence of all key elements of an ISO 31000-based risk management system is examined at the beginning of this study. Then, the quality in terms of efficacy of important aspects of the risk management system is examined in more detail with special benchmarks. The application of the model to six ISO-certified organizations follows and reinforces the novelty of this study, which is to combine risk science knowledge with benchmarking theory in the application of ISO risk management standards in organizations. The results show that the benchmarking model developed in this study provides rigor when assessing and evaluating the efficacy of an ISO risk management system. By applying the model, risk issues and risk factors can be found that had not previously been identified. The findings are of importance for risk management, the benchmarking science, and for the development of ISO risk management standards.

Keywords: risk management; benchmarking; ISO risk management systems; ISO 31000

1. Introduction

Organizations need to adapt to changes and disruptions in their business environment as well as to address internal problems within their structures and operations, such as safety and security. To meet these challenges, organizations apply ISO management systems standards and strive to reach ISO certifications to prove that they have the mechanisms and control structures needed to manage their risk and be resilient in case of a hazard or threat.

ISO defines a standard as a "document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context" [1]. ISO has developed over 24,259 International Standards (https://www.iso.org/standards-catalogue/browse-by-ics.html, accessed on 9 March 2022). There are two types of ISO standards, the management system standards and the guidelines. There are many ISO management standards, and they address problems that cover a wide range of topics, e.g., ISO 9001 quality management [2], ISO/IEC 27001 information security [3], ISO 45001 occupational health and safety [4], ISO 22000 food safety [5], ISO 13485 medical devices [6], and ISO 37001 anti-bribery [7].

It is, however, a potential problem that organizations with ISO certification may feel safe and secure and still overlook or not pay attention to "hidden" risk. There is a need to create benchmarks for ISO standards to address this problem.

This article reports on the development of a risk-oriented benchmarking model based on risk science. It furthermore reports the findings when applied in a real-life case study conducted on six operating organizations, all of which are ISO certified and need to manage their business risk. Being ISO certified means that the organizations rely on ISO management system standards and guidelines, hereafter referred to as ISO standards, as tools for their risk management systems.

The authors' motivation for this study originates in decades of work experience in risk management, from the application of ISO standards in ISO certified organizations, and the auditing of ISO management systems. According to the authors' experience, the application of ISO standards and ISO certifications are no assurance of the efficacy of a risk management system. The risk terminology in ISO standards is not aligned with risk science and the ISO standards give limited guidance on how to analyze, assess, and manage risk [8]. Therefore, the aim of this study was twofold:

1. To develop a benchmarking model for risk management based on scientific literature and ISO standards in order to assess the efficacy of real risk management systems and see whether hidden risk can still be identified through ISO standard risk management systems and the risk assessment process used by operating organizations.
2. To test the benchmarking model on six real-life and ISO-certified risk management systems.

The organizations in this study are all certified by an accredited certification body [9] to at least one ISO management system standard [10], e.g., ISO/IEC 27001 [3], ISO 9001 [2], ISO 14001 [11], ISO 45001 [4], and ISO 13485 [6]. All these standards refer to ISO 31000 [12] as risk management guidelines. Managers of all six organizations were willing to participate in this case study because of increasing business need for analyzing and managing risk. They were interested in finding ways to evaluate the efficacy of their risk management systems in terms of finding hidden organizational risks through the risk assessment process used by the organizations, and to improve their risk analysis technique. Based on a previous study [8], it is hypothesized that certain risk issues will be evident in practice, provided a benchmarking tool (model) can be applied. Examples of such issues are the ability to capture risk in complex systems and that risk criteria can be unclear in ISO risk management systems.

The support and guidance given in ISO standards was investigated from a practical perspective. Testimonials and information provided was evaluated and confirmed through document review and meetings organized as external audits, in accordance with ISO 19011:2018&2011, Guidelines for auditing management systems [13]. The study lasted five years intermittently, from 2014 to 2019. In the meantime, some of the risk management systems evolved and therefore some records were updated, for example, results from risk assessments. Findings in this study take notice of risk management changes made by the organizations until the end of 2019.

The novelty of this study lies in the connection made between risk management systems in businesses and risk science. In addition, benchmarking theory is used to develop a benchmarking model, based on risk issues discussed in recent scientific articles that can be used to assess the efficacy of risk management systems in real ISO-certified organizations. The efficacy of such risk management systems can be difficult to measure because ISO standards are not based on risk science and provide little guidance on how to do so. Due to the growing importance of risk management in all business operations, management, and use of standards, it is important to find ways to measure the efficacy of risk management in a better way than hitherto.

In Section 2, the context for the study is described; in Section 3, the research methodology is illustrated; in Section 4, the results are presented; in Section 5, a discussion on the results is given; and in Section 6, conclusions are drawn.

2. Context for the Study

ISO standards were initially developed as quality standards where the users of the standards define their own quality criteria. Certification audits aim at verifying that the quality is as defined by an organization, whatever it may be. Now that risk management has become an important part of all ISO management systems standards (since 2015) [8,14], the question arises as to whether risk should be treated in a similar way. That is, if the willingness to take risk and the risk taken in ISO certified organizations is entirely the decision of the organizations' managers, and if not, how to evaluate the quality of the risk management. Quality is a unilateral decision of the organizations [15,16], but can risk be treated as a strategic variable like quality? The risk must be identified and understood to be able to assess it and decide if and how it should be treated. Here, the application of the standards varies regarding risk and quality, and, for example, auditors face a challenge when evaluating a risk management system. Managing risk and auditing risk management systems requires knowledge of risk management, often expert knowledge on risk analysis techniques on one hand and the subject facing risk on the other hand (e.g., design, development, production, services, operations). According to the authors' knowledge, no formal benchmarking models have been used until now as tools to evaluate the efficacy of ISO risk management systems.

Section 2.1 reviews recent developments influencing the development of benchmarking models regarding ISO standards. Section 2.2 reviews the risk management guidelines in ISO 31000, the structure, and use of the standard. Section 2.3 reviews selected scientific literature on risk issues in risk management systems, selection based on findings in recent article on risk management guidelines [8]. Section 3 describes the development of a benchmarking model used in this article for reviewing and evaluating the six real-life ISO risk management systems in this study.

2.1. Recent Developments Influencing the Development of Benchmarking Models

The Cambridge dictionary defines benchmarking as "the act of measuring the quality of something by comparing it with something else of an accepted standard" (https://dictionary.cambridge.org/dictionary/english/benchmarking, accessed on 9 March 2022). Benchmarking is therefore an important tool to help organizations to continuously improve the quality of their products and services. It is a popular tool in industry [17–20], but it is also used in the health service to improve patient outcome, for example in surgery [21]. In this study, the quality is limited to the efficacy of the risk management system. The Cambridge dictionary defines efficacy as "the ability [. . .] of a method of achieving something, to produce the intended result". In this, section some examples of benchmarking contributions will be reviewed.

Herbst et al. [17] discuss benchmarking in cloud computing, which in recent years has become a significant part of information and communication technology. Benchmarks play an important role as evaluation tools during system design, development, and maintenance. They are therefore the basis for informed decisions. Herbst et al. lay a foundation for benchmarking cloud computing settings, one of which is operational risk. They use risk as a quality aspect reflecting the impact of running an application in cloud infrastructures and define operational risk as a group of metrics determining the risk of production systems running in cloud environments.

Kounev et al. [18] expand the discussion on benchmarking in information and communication technology in their book "Systems Benchmarking—for Scientists and Engineers" on the theory and practice of benchmarking. Due to the increasing importance of risk management, risk management benchmarking has now become an important research field. Kounev et al. discuss how benchmarks play an integral part in the evaluation and validation of new approaches and methodologies in research. The book focuses on the benchmarking of systems and components used as building blocks of modern information and communication technologies applications. In traditional benchmarking, the emphasis has been on evaluating performance, generally understood as useful work accomplished by

a system (or component) compared to the time and resources spent. Kounev et al. describe how performance benchmarks have contributed significantly to improve successive generations of systems. They describe how research on dependability benchmarking has increased beyond traditional performance benchmarking in the past two decades. They also note that resilience benchmarking faces challenges related to the integration of dependability, performance, and security benchmarking as well as to the adaptive characteristics of the systems under consideration.

Olawumi and Chan [19] present a study on the development of a benchmarking model for information modeling for buildings. This concerns "a repository of digital information which facilitates the efficient management of project information from conception by way of simplifying and presenting a real-world simulation of a pre-conceived project facility". A qualitative approach was used to form the foundation of the proposed model. An assessment template and scoring system were developed to support the benchmarking model by providing a quantitative metric system for the proposed model. Olawumi and Chan conclude that construction organizations and project teams can benefit from the benchmark model and use the template and the associated scoring system to assess the level of information modeling innovation for buildings. They also conclude that their benchmarking model helps validate the implementation of the best practice framework in a project and improve the management of project information throughout the building lifecycle.

Van der Voordt and Jensen [20] compare the benchmarking theory and performance measurement with current practice and data from different work environments. To add value to an organization, workplaces must provide value for money by a positive trade-off between the benefits. They must support the organizational objectives and processes, with regard to the cost, time, and risk connected with achieving these benefits. They find that both quantitative and qualitative performance indicators, including hard and soft factors, are needed to define the trade-off between the costs and benefits of interventions in corporate real estate, facilities, and services, and to cope with the interests and needs of different stakeholders. Risk and risk expenses are amongst the value parameters they discuss.

Staiger et al. [21] address application and improvements in health care through benchmarking. They propose a systematic benchmarking approach in surgery, including the establishment of best achievable postoperative outcomes. According to Staiger er al., a standard approach for determining benchmarks enables self-assessment in surgical outcome and helps detect improvement opportunities. They emphasize that the intention of benchmarking in surgery is to stimulate surgeons' genuine endeavor for perfection, rather than to criticize the surgeons' performance or the health service. The goal must however be the improvement in patient outcome. They mention that new benchmarks should be defined in connection with high-risk groups, risk profiles, and risk adjustment.

Hartono et al. [22] discuss models for benchmarking qualitative data. In data envelopment analysis, performance evaluation is generally assumed to be based on a set of quantitative data. When evaluating processes or making decisions, it is, however, often necessary to take qualitative factors into account. They mention that some qualitative data measurement approaches have disadvantages when assessors provide judgment and cannot model the computational trust considering hesitancy, vagueness, and uncertainty. They propose a "hesitant fuzzy linguistic term sets" model which provides value for both input and output of decision maker units, based on a qualitative and sometimes hesitancy-based assessment. The results of Hartono's and Abdullah's study indicate that in data envelopment analysis the assessor can perform a good assessment in the form of qualitative data on the input and output of each decision maker units and then evaluation results will be available for use in the benchmarking process with the data envelopment analysis.

Mangla et al. [23] explore the relationship between various risk management strategies and practices in order to design and thus enact a suitable plan for supply chain risk mitigation. They discuss benchmarks for green supply chain managers and planners to help them model and assess risks and possible failures associated with their work. They use fuzzy failure mode and effects analysis approach to identify and assess the risks

associated with green supply chain. Mangla et al. conclude that their findings will help companies to reduce risk and its consequence, but also in enhancing its ecological-economic business sustainability.

Hoffmann et al. [24] study the antecedents of supply risk management performance. They use speed consortium benchmarking to explore the concepts of supply risk monitoring and mitigation. They identify not only the antecedents of supply risk management performance, but also the moderating effect of different supply risk management principles on the relation between uncertainty and supply risk management performance. Their study shows the relevance of developing general risk management structures and capabilities (i.e., risk management process maturity) to manage risk successfully. Their findings indicate that the implementation of a risk management process is even more important than the proper selection of individual risk monitoring and mitigation strategies.

Björklund [25] presents the development of a benchmark tool that can be applied to improve corporate social responsibility in purchasing. The tool was tested on two organizations which illustrates how the benchmarking tool can be applied. It provides a simple and systematic approach for evaluating a company's performance, improves transparency, and enhances cross-company comparison. The benchmark tool addresses both quantitative and qualitative aspects. Björklund concludes that it is of large importance to combine quantitative and qualitative measures in this area as quantification can be misleading if used in isolation.

Moriarty and Smallman [26] conduct a study on the theory of benchmarking. In their article, they review the epistemology of benchmarking and identify methodological elements of the theory of benchmarking. They discuss critiques of benchmarking which focus on three areas: (1) information (the reliability of exemplar information); (2) implementation (the intangibilities associated with implementing benchmarking); and (3) theory (the lack of a theoretical framework that distinguishes effective from ineffective efforts). This critique detracts from the potential advantages benchmarking appears to offer. The literature review they conduct shows overwhelmingly pragmatic approaches to benchmarking (that is, process-driven, case-oriented, and generic) as opposed to theoretical. Where theories are referred to, they center on the utility of benchmarking in terms of organizational learning and reasoning as well as economic enhancement.

MacGillivray et al. [27] describe the application of a capability model to benchmark the risk management maturity of eight water utilities in different countries. Their analysis codifies risk management practice and offers practical guidance on how utilities can more effectively use various risk analysis techniques for optimal, credible, and defensible decision making. Their case study shows that good risk analysis practices include: (a) use of initiation criteria for applying risk assessment techniques; (b) the implementation of formalized procedures to guide their application; (c) peer reviews; and (d) auditing. This ensures procedural compliance and provides quality assurance. MacGillivray et al. also identify common weaknesses, likely to be representative of the water utility sector they covered in their study, notably a need for improved risk knowledge management, education, and training in the discipline.

The examples of benchmarking contributions reviewed in this article describe various challenges, recent developments, and issues that are important for state-of-the-art benchmarking. The literature confirms the importance and challenges of benchmarking in the assurance of quality in risk management. The results can be summarized as follows:

1. Benchmarking is important for risk management [17,18,20,21,23,24,27].
2. Benchmarking is an important tool for performance evaluation and improvement processes of organizations [17–20,22,25,26].
3. In benchmarking, it may be necessary to combine quantitative and qualitative factors [17–20,22,25,26].
4. A scoring system helps in defining and verifying the "quality" of risk management actions [19,22,27].

5.   A benchmarking system can be applied to stimulate a genuine endeavor for perfection, rather than to judge or criticize [21].

2.2. Risk Management in ISO Standards

ISO 31000 [12] is the main ISO guideline for risk management and according to ISO the standard "provides a common approach to managing any type of risk and is not industry or sector specific" (https://www.iso.org/standard/65694.html, accessed on 9 March 2022). It is intended for general guidance on risk management systems and not for certification. The first version of the standard was published in 2009 and this case study was originally based on that version. In an updated version, published in 2018, the principles of risk management have been reviewed. Greater emphasis is put on leadership by top management to ensure that risk management is integrated into all organizational activities, starting with the governance of the organization [28]. Greater emphasis is also put on the iterative nature of risk management, drawing on new experiences, knowledge, and analysis for the revision of process elements, actions, and controls at each stage of the process. According to the standard, risk management is based on the principles (described in clause 4), framework (described in clause 5), and process (described in clause 6). This is illustrated in Figure 1.
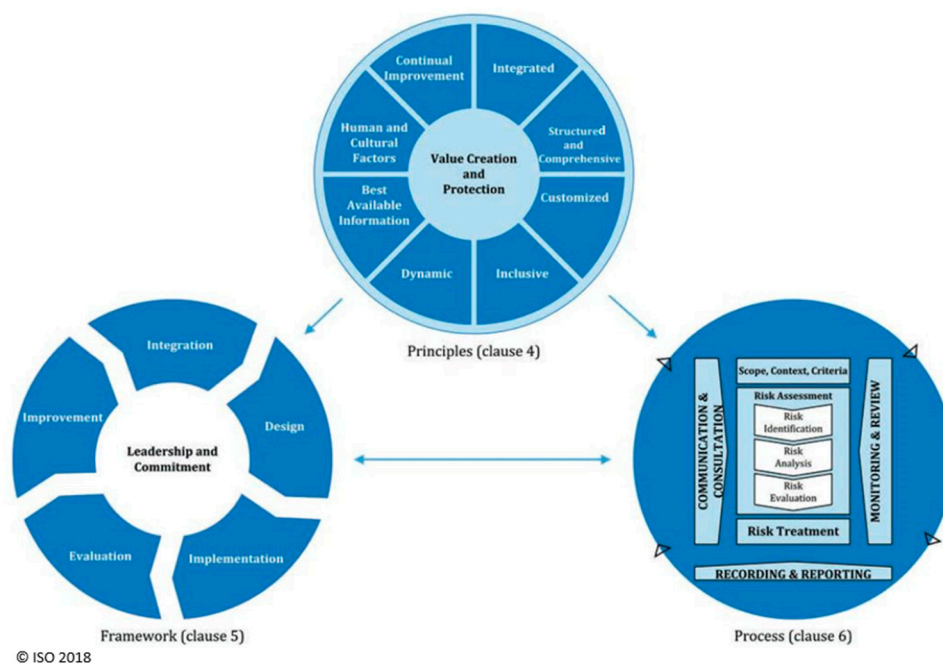
Figure 1. Graphical illustration of risk management from ISO 31000:2018 [12], principles, framework and process. Figure published with permission from Icelandic Standards.

The principles are the foundation for managing risk and should be considered when establishing the risk management framework and processes of an organization. The purpose of the risk management framework is to assist the organization in integrating risk management into activities and functions. The effectiveness of risk management depends on its integration into the governance of the organization, including decision making [29]. The components of the framework should be customized to the needs of the organization. Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all the organization's activities, including decision making. The risk management process involves the systematic application of the policies, procedures, and practices to the activities of communication and consulting, defining the scope and establishing the context, assessing, and treating risk, monitoring, reviewing, recording, and reporting risk. Risk criteria should be aligned with the risk management framework and customized to the specific purpose and scope. It should reflect the orga-

nization's values, objectives, and resources, and should be consistent with policies and statements about risk management.

The ISO 31000 standard only contains guidelines, not requirements. The guidelines do not contain benchmarks for risk management in general, nor individual elements of the risk management principles, framework, or process. When auditing risk management systems that are based on ISO standards, the auditors apply the auditing standard ISO 19011 [13]. This standard is a general auditing standard, aimed at the auditing process itself and does not include benchmarks for risk management. The auditor is meant to seek written evidence (proof) of risk management, for example, the risk management process. The requirements are to be found in the ISO management system standard, such as ISO 9001 [2], ISO/IEC 27001 [3], ISO 45001 [4], ISO 13485 [6], and ISO 14001 [11].

In this study, the risk management process, as described in Figure 1, is used as a basis for benchmarking the risk management process in Section 3. The requirements regarding the risk management are obtained from ISO/IEC 27001, ISO 45001, and ISO 13485, and can be summarized as follows:

1. The scope of the risk management system must be defined.
2. The risk management process must be documented.
3. Policies regarding risk management must exist and be documented.
4. Internal audits must be conducted.
5. Management review and formal review and approval for suitability and adequacy, for example, review of operational planning and control, assessments of risk, nonconformity, and the efficacy of any corrective action taken.
6. Knowledge of all legal requirements must exist.
7. Risk and root cause analysis must be conducted.
8. Risk assessment/evaluation must be conducted.
9. Criteria must be set for the management system process and risk/quality acceptance.

When a requirement is required to be "documented" in an ISO standard, it is required to be established, implemented, and maintained. The requirements of ISO 9001 and ISO 14001 are less clear regarding risk management and it is not possible to build specific benchmarks on them [30].

2.3. Scientific Literature on Risk Issues in Risk Management Systems

Risk management systems, as described in ISO 31000, consist of risk management principles, framework, and process. According to ISO 31000, it is in the risk management process where the identification and evaluation of risk takes place, see Figure 1. The scientific basis of ISO risk management standards has been questioned in recent scientific literature [8,31–33]. ISO standards do not reference scientific literature, only other ISO standards and sometimes risk assessment techniques and handbooks. The only bibliographic reference in ISO 31000 is IEC 31010 [34]. IEC was first published in 2009 and then updated in 2019. It is a dual logo IEC/ISO standard for supporting ISO 31000. It provides guidance on the selection and application of systematic techniques for risk assessment. Some changes have been made regarding bibliographic references in the latest version of IEC 31010:2019. In version 2009, only 11 bibliographic references were made, all to other ISO/IEC standards. In the 2019 version, there are 91 bibliographic references. Many of them are not standards but handbooks and they are categorized in the bibliography according to risk techniques with no direct reference to risk science. Therefore, the aim of the literature review in this section is to identify risk issues that are the subject of scientific literature but not addressed in ISO standards. In this section, some examples of risk management science contributions are reviewed, as the basis for definition of benchmarks for a generic risk management process in Section 3.

Björnsdóttir et al. [8] conducted a review of 18 ISO standards (including ISO 31000, ISO/IEC 27001, ISO 45001, ISO 13485, ISO 9001, and ISO 14001) with regard to risk management to find out how well aligned the ISO standards are with scientific literature. Their study also aimed at evaluating if and how the standards address the management of risk

arising from complex interactions and emergent behavior that is inherent in present-day socio-technical systems. The study shows that ISO standards are not based on risk science and there are inconsistencies in both risk terminology and risk management guidelines. It also shows that it is difficult to standardize many risk-related factors, for example, the assessment criteria for something that is intangible. Björnsdóttir et al. show that ISO standards do not support users appropriately in analyzing and assessing risk when it comes to the complexity of socio-technical systems, emergent behavior, and non-linear causal relations.

Aven and Zio [31] analyze the foundational issues of risk assessment and management in their article. They discuss the needs, obstacles, and challenges for the establishment of a renewed, strong scientific foundation, suited for the current and future technological challenges. Among the issues Aven and Zio identify is terminology and fundamental principles; the risk management field lacks universally understood and well-defined terms. They also point out that risk analysis of critical infrastructure systems, e.g., power grids, is both challenging and important. Such systems are often complex and interdependent where system components interact on multiple scales of space and time. The system components are often heterogeneous and form a hierarchy of subsystems. There is a need for appropriate tools and techniques for analyzing risk and vulnerabilities in such complex systems. Furthermore, they mention issues regarding the scope and science of risk assessment and point out that quantitative risk assessment methods need to cover knowledge (description and characteristics) of the uncertainties.

Klinke and Renn [32] discuss a new approach to risk evaluation and management. They propose a new classification of risk types and management strategies for dealing with the problems of complexity, uncertainty, and ambiguity—with scientific accuracy, a reflection of social diversity, and political feasibility. This includes criteria for evaluating risk and a classification of risk types and risk management strategies. Their concept of risk evaluation criteria, risk classes, a decision tree, and management categories was developed to improve the effectiveness, efficiency, and political feasibility of risk management procedures. The main task of risk evaluation and management is to develop adequate tools for dealing with the problems of complexity, uncertainty, and ambiguity.

Cox [33] discusses the uncertainty involved in the use of risk matrices, which is a widespread way of assessing risk. The meaning of a risk matrix may be far from transparent, despite its simple appearance. Cox examines some mathematical properties of risk matrices and shows that they have the following limitations: (a) poor resolution; (b) errors; (c) suboptimal resource allocation; and (d) ambiguous inputs and outputs. He demonstrates that, in general, quantitative and semiquantitative risk matrices have limited ability to correctly reproduce the risk ratings implied by quantitative models, especially if risk components such as frequency and severity are negatively correlated. Cox suggests caution in using risk matrices because they do not necessarily support good risk management decisions.

Aven [35] also addresses the weaknesses of risk matrices. They are a common practice for the characterization of risk, reflecting threats and their consequences and probability, as well as concepts such as risk factors and sources. His conclusion is that risk matrices in the traditional two-dimensional consequences-probability form should not be used. Such matrices need an additional knowledge dimension to capture and include the strength of knowledge judgements and rankings of risk factors and assumptions supporting the analysis.

Fellows and Liu [36] discuss boundary issues across multiple interfaces in engineering construction projects. Such projects have many boundaries between various stakeholders. According to Fellows and Liu, organizations engaged in such projects require permeable boundaries to allow information flow, knowledge sharing, and learning so that they can respond appropriately and quickly to changes. Thus, while formal boundaries may be fixed and rigid, informal boundaries in projects may need to be flexible and facilitate organizational adaptations for performance of constituent project activities, especially in project governance. The main concern here is to nurture cooperation, collaboration,

and commitment with respect to the diverse natures and interests of the participants. Complexity issues also arise through increasingly complex projects and their organizational structures. A high degree of specialization often needs the involvement of numerous specialized companies, each of which has its own boundary. The performance and success depend on how well the boundary activities are planned and managed. Fellows and Liu conclude that engineering construction projects are nested hierarchies of complex adaptive systems involving numerous, diverse stakeholders. Thus, performance requirements and parameters are emergent. The systems co-evolve, and any equilibria are dynamic.

Mikes [37] discusses boundary issues and work in risk management. Her field study in the banking sector suggests that the boundary work of risk experts advances two different approaches to risk management, depending on their calculative cultures. The financial crisis of 2007–2009 proved to be a challenge to risk management in the banking systems. Since then, the risk experts have tried to find ways to improve risk management. On one hand, there is a culture of quantitative enthusiasm, where risk functions are dedicated to risk measurement. On the other hand, there is a culture of quantitative skepticism, focusing on envisioning risk and aiming to provide top management with alternative future scenarios and with expert opinions on emerging risk issues. The study shows that those displaying quantitative enthusiasm strived to capture the complexity of risk decisions. As much judgment as possible is included upfront in the model design, so that the output of the model could be regarded as a close proxy to the underlying risk profile. Again, senior risk managers with a strong quantitative skepticism expanded the boundaries of the risk universe (all risk that could affect an entity) beyond modeling by creating fora for the envisioning of non-calculable risk objects. They relied less on formal models than on their own cognitive mental models, imagining alternative futures about which the existing models had nothing to say. They sought to anticipate emerging risk and uncertainties that are not measurable in order to guide discretionary strategic decisions, for which they were ready to take responsibility. Mikes discusses that "if risk officers are to uphold the ideal of measurement, they can only extend their remit to risks that can be described by a priori known or statistically knowable distributions. Alternatively, if they are to discuss and influence the management of non-quantifiable risks, threats, and opportunities (Knightian uncertainties), they have to venture outside the measurement framework". She concludes that as risk management practitioners move forward in their work, theoretical and empirical researchers will be summoned to account for new realms, new definitions, and new purposes of risk management.

Zerjav [38] addresses the problem of boundary dynamics and issues of resources allocation in infrastructure projects. Due to their complexity and high social impact, such projects often face challenges in managing the design decision-making processes across disparate disciplinary and knowledge domain boundaries. Zerjav identifies the key role of resource allocation constraints, path dependency of project decisions, and problem-solving nature of design. He introduces the notion of design boundary dynamics for describing diverse cross-boundary coordination phenomena associated with organizing the design of infrastructure projects.

Lathrop and Ezell [39] address the validation of risk analysis. They describe, with a systems approach, that validation of a risk analysis should be based on how well the risk analysis supports risk management. When assessing how well the risk analysis supports risk management, it should be considered how well it supports the decision-making process. They conclude that the implementation of risk management actions results in what matters: the final consequences and residual risk.

The risk issues addressed in the literature can be summarized as follows and applied as benchmarks as presented in Section 3:

1. Scope and outer boundaries of a risk management system [31,36–38].
2. Interfaces (internal boundaries, departments, unclear responsibility) within a risk management system [31,36–38].

3. Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a risk management system [31,36].
4. Resources available to support a risk management system [33,38].
5. Risk analysis ability to capture complex systems and business operations [8,31,32,36–38].
6. Risk assessment ability to capture risk evaluation, e.g., with risk matrices [8,32].
7. Risk criteria setting in risk assessment [8,32].
8. Treatment of residual risk [39].

3. Development of a Benchmarking Model for an ISO Risk Management System

The benchmarking model developed and applied in this research is based on the literature review and context of the study as described in Section 2. It is divided into the following two steps:

Step 1: Validation and evaluation of the foundational elements of a generic risk management system that is based on ISO standards. Assessment template with a simple scoring system.

Step 2: Validation and evaluation of some of the most critical elements of the risk management process, according to ISO and scientific literature on risk management issues.

3.1. Step 1

An assessment template with simple scoring system can be used to evaluate the existence of the basic elements of a risk management system. Based on the findings in Sections 2.2 and 2.3, the following benchmarks were defined. The scoring system provides a quantitative metric system with simple scores such as "yes", "no", "not applicable", and "not specified". The proposed benchmarks are as follows:

1. Scope, context, and boundaries of the risk management system.
2. Compliance with regulative requirements concerning the business.
3. Certifications.
4. Policies regarding risk are documented.
5. Risk management system is documented.
6. Risk analysis is conducted in a formal way.
7. Risk assessment is conducted in a formal way.
8. Risk (acceptance) criteria are set.
9. Residual risk is addressed (identified and assessed).

3.2. Step 2

If a risk management system meets the criteria in Step 1 and the benchmarks are positive, the next step is to assess the quality in terms of efficacy of individual elements of the risk management system. In this study, the most important elements of the risk management process were put in focus and findings in Section 2.3 used as basis for benchmarks.

To assess the scope further, context, compliance, and conformity of the risk management system (no. 1–5 in Step 1), the following benchmarks were defined:

1. Scope and outer boundaries of the risk management system.
2. Internal boundaries and interfaces, complexity of the organizational structure, and distribution of accountability.
3. Hierarchical structure with regard to risk, both safety and security risk.
4. Resources, knowledge, and experience needed to support the risk management system.

Additionally, the following benchmarks were defined to further assess the efficacy of some of the most important elements of the risk management process (no. 6–9 in Step 1):

5. Risk analysis ability to capture complexity of the business operation and systems (foundation, method, technique).
6. Risk assessment ability to capture risk evaluation (ability to capture risk knowledge).
7. Risk criteria setting in risk assessment.

8. Identification and treatment of residual risk, risk that is left after formal risk mitigation/treatment.

Table 1 gives an overview of the benchmarks in Step 2. The first column shows the benchmark number, second column shows the benchmark name, third column shows the corresponding principle/framework/process in ISO 31000 as described in Section 2.2.

Table 1. Benchmarks with correspondence to ISO 31000:2018 [12].

No.	Benchmark Name	Corresponding Risk Management (RM) Principle/Framework/Process Clause in ISO 31000
1	Scope and outer boundaries of a RM system	Process (clause 6): Scope, context, and criteria (6.3)
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Process (clause 6): Scope, context, and criteria (6.3)
3	Hierarchical issues (layer issues, unclear hierarchical safety and security structure) within a RM system	Principles (clause 4): Structured, comprehensive, and dynamic RM Framework (clause 5): Leadership and commitment (clause 5.2) Process (clause 6): Risk assessment (clause 6.4) and risk treatment (clause 6.5)
4	Resources available to support the RM system	Framework (clause 5): Leadership and commitment (clause 5.2)
5	Risk analysis ability (foundation, method) to capture complexity	Process (clause 6): Risk assessment (clause 6.4)
6	Risk assessment ability to capture risk evaluation	Process (clause 6): Risk assessment (clause 6.4)
7	Risk criteria setting in risk assessment	Process (clause 6): Risk assessment (clause 6.4) and risk treatment (clause 6.5)
8	Treatment of residual risk, risk that is left after risk mitigation	Principles (clause 4): Continual improvements Framework (clause 5): Improvement (clause 5.7) Process (clause 6): Risk assessment (clause 6.4), risk treatment (clause 6.5), monitoring and review (clause 6.6)

4. Research Methodology and Hypotheses

After developing the benchmarking model described in Section 3, this research proceeded in the following five steps: (1) setting selection criteria for participants in the study; (2) selection of business sectors and organizations; (3) conducting of a risk management questionnaire based on the benchmarking model in Step 1; (4) follow-up interviews; (5) evaluation of the risk management process applying the benchmark model developed in Step 2. Figure 2 gives an overview of the research process. It describes the research methodology and its individual steps, also reflecting the structure of this article. The next two subsections describe the research methodology (Section 4.1) and the hypotheses put forward (Section 4.2).
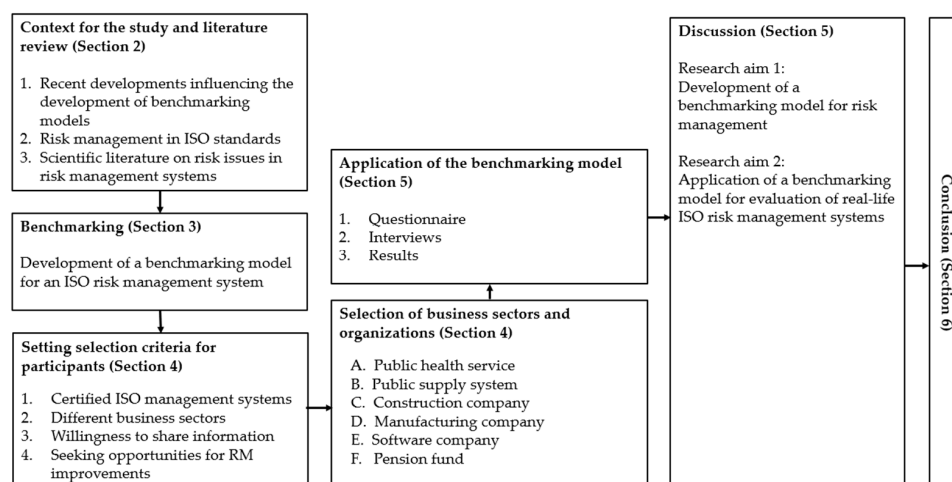
Figure 2. Research overview.

4.1. Research Methodology

4.1.1. Setting Selection Criteria for Participants in the Study

A desk study was conducted to define selection criteria and identify possible candidates for the research. Eligibility criteria were specified. The organizations should: (a) have a certified ISO management system, or at least be in the implementing phase of an ISO management system; (b) be from different business sectors; (c) be willing to share information from what were considered to be successful business operations or projects; (d) be seeking opportunities to improve their risk management process in general.

Organizations operating in six industry sectors were selected: (A) public health service; (B) public supply system; (C) construction company; (D) manufacturing company; (E) software company; and (F) pension fund. Table 2 shows a list of the organizations selected for this case study. The first column shows the organizations' type of business. The second column shows the business operations examined in this study. The third column shows the ISO standards each organization is certified to.

Table 2. Organizations examined in this study.

ID	Organization	Business Operation	Accredited ISO Certifications
A	Public health service	Processing of biological samples	ISO 9001
B	Public supply system	Operation of an electricity transmission system	ISO 9001, ISO 14001, ISO 45001
C	Construction company	Construction of an infrastructure facility	ISO 9001, ISO 14001, ISO/IEC 27001, ISO 45001
D	Manufacturing company	Manufacturing of a medical device	ISO 14001, ISO 13485
E	Software company	Software development	ISO/IEC 27001
F	Pension fund	Financial investments	ISO 9001, ISO/IEC 27001

All six organizations fulfil the research criteria mentioned above. Five of them already had accredited certification to one or more ISO standards when the case study started in 2014, one was in the implementing phase and received accredited certification during the time of the study, end of 2018. Written contracts were made with all organizations to ensure information security according to the requirements of ISO/IEC 27001:2013 [3] throughout and after the case study process. A contact person was nominated in every organization, responsible for the delivery of information, orally and written. After signing contracts and confidentiality agreements, meetings were held with the contact persons and their teams to inform them, explain the aim of the research, answer questions, and clarify expectations on both sides.

4.1.2. Questionnaire

The questionnaire (see Table 3) is based on the research framework described in Section 3. It was sent to the contact persons in each organization. Answers from questionnaires along with supporting documents (e.g., organizational manuals, description of processes and procedures, policy documents, and results from risk assessments) were received from all organizations. These data were reviewed with regard to benchmarks, content of information, and alignment with guidelines in ISO 31000.

Table 3. Questionnaire summary.

No.	Question/Topic	A—Public Health Service	B—Public Supply System	C—Construction Company	D—Manufacturing Company	E—Software Company	F—Pension Fund
1	**General information**						
1.1	Listed (on Nasdaq)	no	no	no	yes	yes	no
1.2	Number of employees (European Union classification)	51–250	51–250	251–500	501–5000	11–50	11–50
1.3	Number of local sites/offices	4	2	7	1	1	1
1.4	Number of countries with subsidiaries	1	1	1	18	2	1
1.5	Intl. business operations and export	no	no	yes	yes	yes	yes
2	**Compliance**						
2.1	Relevant laws and regulations for business identified	yes	yes	yes	yes	yes	yes
3	**Certification**						
3.1	Operations ISO certified	all	all	all	partly	all	all
3.1.1	. . . if yes, by an accredited certification body	yes	yes	yes	yes	yes	yes
3.1.2	. . . if yes, name of certification body	list	list	list	list	list	list
3.2	Non-ISO certifications	yes	no	yes	yes	no	no
3.2.1	. . . if yes, which parts	list	list	list	list	list	list
3.2.2	. . . if yes, which accredited certification body	list	list	list	list	list	list
4	**Policies**						
4.1	Safety and/or security policy exist	yes	yes	yes	yes	yes	yes
4.2	Documented safety and/or security policy exists	no	yes	yes	yes	yes	yes
4.3	Ref. to relevant law(s)/regulation(s) in policy documents	list	list	list	list	list	list
4.4	Other policy documents relevant to safety/security	yes	yes	yes	yes	yes	yes
5	**Risk management system**						
5.1	Formal risk management process in place	yes	yes	yes	yes	yes	yes
5.2	Risk assessment conducted	yes	yes	yes	yes	yes	yes
5.3	Risk analysis conducted	yes	yes	yes	yes	yes	yes
5.4	Internal control	yes	yes	yes	yes	yes	yes
5.5	Audits, internal and/or external	yes	yes	yes	yes	yes	yes
5.6	Review process	yes	yes	yes	no	yes	yes
6	**Risk analysis**						
6.1	Formal methodology used	yes	yes	yes	yes	yes	yes
6.2	Use of special software solution for risk analysis	no	yes	no	no	yes	no
6.3	ISO guidelines used for doing risk analysis	no	yes	yes	yes	yes	yes
6.4	Likelihood of risk assessed	no	yes	yes	yes	yes	yes
6.5	Risk evaluated	yes	yes	yes	yes	yes	yes
7	**Risk assessment**						
7.1	Tangible assets registered	yes	yes	yes	n.a.	yes	yes
7.2	Intangible assets registered	yes	yes	yes	n.a.	yes	yes
7.3	Threats identified	yes	yes	yes	n.a.	yes	yes
7.4	Consequence of risk assessed	yes	yes	yes	yes	yes	yes
7.5	Risk calculated	no	yes	yes	yes	yes	yes
7.6	Systematic risk mitigation with controls	yes	yes	yes	yes	yes	yes
7.7	Risk calculation after selecting controls—efficacy of controls assessed	no	yes	n.s.	no	yes	yes
7.8	Assessment on efficacy and usefulness of risk analysis in terms of cost	no	yes	yes	no	no	no
7.9	Risk information used for improvements—someone responsible	yes	yes	yes	yes	yes	yes
7.10	Result of risk assessment documented	yes	yes	yes	yes	yes	yes
7.11	Result of risk assessment used to learn from it	n.s.	yes	yes	yes	yes	yes
8	**Risk criteria**						
8.1	Risk criteria set	no	yes	yes	yes	yes	yes
9	**Residual risk**						
9.1	Residual risk assessed	no	yes	no	yes	yes	yes

"list" = list provided; "n.a." = not applicable; "n.s." = not specified.

4.1.3. Interviews

After collection, review, and analysis of data from the questionnaire, follow-up meetings were organized and held as audit meetings according to ISO 19011 [13]. The aim was to confirm the information given in the questionnaire. This was done by obtaining evidence, review, and confirming data integrity and compliance with records received. Records on incidents and nonconformities were reviewed and the efficacy of the ISO plan-do-check-act cycle was examined with regard to corrective actions. Meetings were recorded where permission for recording was obtained. The follow-up meetings led to a variety of findings. Subsequently, more information and evidence were gathered, and testimonies recorded. The case study lasted five years intermittently. In the meantime, some of the organizations developed their risk management systems and therefore some records (e.g., results from risk assessments) were updated.

4.2. Hypothesis

Since all participants in this real-life study are certified to ISO management system standards that require risk management, it can be expected that all major aspects of risk management are present and for the most part well documented. However, ISO standards lack guidance on risk management as demonstrated by Björnsdóttir et al. in a previous study [8]. Consequently, it is expected that risk management, and particularly the analysis of risk, is executed in an unsatisfactory manner. Assuming that the representatives of the organizations in this study are describing the true situation in their organizations, it is therefore hypothesized that certain flaws in risk management will be evident in practice. The benchmarks developed, based on the literature review conducted in Section 2.3 and presented in Table 1, are used to evaluate the risk management systems examined in this study.

5. Results

The results of this study are presented in the following six subsections, one section for each organization. The results are presented in tables and discussed, and conclusions drawn. An overview of the results from the questionnaire is presented in Table 3. The topics/questions are grouped into categories, intended to:

1. Capture general information regarding the business operations and the risk management system: scope, interface, organizational structure (hierarchy and layers), and resource issues. This is consistent with topics no. 1–4 in Table 3 and benchmarks no. 1–4 in Table 2.
2. Capture more specific information about the risk management system: foundational issues, risk analysis technique, ability to capture complex risk, ability to evaluate risk, including residual risk. This is consistent with topics no. 5–9 in Table 3 and benchmarks no. 5–9 in Table 2.

The first two columns show the number and name of question/topic in the questionnaire. The following six columns show the results for individual organizations. The results are examined and explained in the next six subsections, one subsection for every organization. In most cases, the answers are "yes" or "no". The answer "list" means that a list was provided, "n.a." means not applicable, and "n.s." means not specified.

5.1. Public Health Service

The public health service (organization A in Table 2) is an independent part of a university hospital. It is responsible for the processing of biological samples, e.g., blood. The main operations are in the hospital area, but it also has two sites outside the main hospital area and a mobile sample collection unit. The service of the organization includes collecting and processing of blood, testing, education, services regarding cells and tissues, transplantation, and stem cell therapy. Part of the infrastructure, e.g., information technology support and technical assistance, is in the hospital's organizational chart under a different management system. During the time of this study, the contact person moved on from being a quality

manager to becoming head of department. The risk management system developed in such a way that risk analysis has become a part of all working procedures, which was not the case at the beginning of the study.

5.1.1. Results from the Questionnaire

The public health service is certified to ISO 9001 [2] to ensure the correct working procedures, quality, and safety of the products and services. It also has other types of specific certifications and operating licenses not related to ISO. The quality policy is documented and addresses both safety and security, but no other ISO management system policy documents exist. There is good knowledge of the legal environment. A formal risk management process is in place, as a part of the ISO management system. This means that risk assessment and risk analysis are conducted, there is internal control, regular audits (internal and external), and a management review process. A formal risk analysis technique is used in the form of a two-dimensional risk matrix in Excel. ISO risk management guidelines are not used, both tangible and intangible assets are identified, and risk is related to assets. Threats to assets are identified, and consequence of risk assessed. Likelihood of risk is not a factor in the assessment, risk is not calculated, risk criteria are not set, and residual risk is not assessed.

5.1.2. Results from the Interview

The head of department (former quality manager) of the public health service was interviewed. The interview revealed that risk management of the organization is mainly based on international health science norms and standards published by the European Commission and the World Health Organization, and not on ISO standards. One of these guidelines is the Guide to the Preparation, Use, and Quality Assurance of Blood Components [40]. The World Health Organization, WHO, has also published international health science norms and standards, e.g., the WHO Action Framework to Advance Universal Access to Quality and Safe Blood and Blood Components for Transfusion and Plasma Derived Medicinal Products [41]. These publications define hazards within the health service environment. For example, the most hazardous states regarding blood processing involves blood leaving the organization with one or more of the following hazards: (a) blood is mislabeled; (b) contaminated blood passes screen; (c) blood spoils within the organization.

Risk analysis is conducted on many levels and is not based on ISO 9001, since there is no guidance on risk analysis in the standard, and only partly based on ISO 31000. In case of blood donation, the risk analysis starts when a blood donor comes to the organization. A healthcare professional interviews the donor and assesses his or her suitability for donation. The assessment is documented. Another part of the risk assessment is the quality control process of blood components, based on content and sample requirements. The quality control is done by trained healthcare professionals, records are made in Excel sheets and in a database. Risk assessment is also done as a part of an incident registration process, which includes a review and evaluation of an incident. However, work is not always done according to that process. A two-dimensional risk matrix is used to assess an incident and determine a risk factor, based on impact of risk and likelihood of recurrence, both on a scale of 1 to 5. Three different colors (green, yellow, red) are used to show the severity of a risk factor. The risk analysis became more formal after this study started and at the end of it, more employees had been mobilized to take part. There are risk issues regarding, e.g., information technology support and assistance, which is not a part of the risk management system of the organization but a part of the hospital's central infrastructure.

The interview also revealed that there are risk factors that have not been registered or formally assessed. The department head is aware of these risk factors but has not found a way to either assess them or treat them because they are on the border of the business scope. This risk is related to the delivery and use of blood products and cooperation with health organizations receiving blood products, but not having a formal quality or risk management

system themselves. There are also risk issues in interactions and communications with health authorities that has neither been registered nor treated.

5.1.3. Summarized Results from the Public Health Service

The public health service is an important part of the infrastructure of the health system. It is not a competitive business entity, but the ISO certification shows ambition in operation and good service. The procedure for risk analysis is not yet fully documented. It is difficult to manage risk on the border of the business scope and risk related to communication. Lack of communication with external parties has been difficult to capture. It has also been difficult to communicate risk information to authorities. Table 4 presents a summary of the results from the public health service.

Table 4. Results from the public health service.

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	Outer boundaries of RM system stretched into other health care institutions without compliance with ISO procedures	True
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Boundary issues regarding joint service and infrastructure of the hospital	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Two-dimensional risk metrics does not capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk criteria unclear	True
8	Treatment of residual risk	Residual risk not addressed	True

5.2. Public Supply System

The public supply system (organization B in Table 2) transmits electricity from generation stations to regional electricity distribution operators and power intensive users by way of a high voltage transmission system (power grid). The operation is regulated by the national energy authority which determines the revenue cap on which the electricity tariff is based. The public supply system is a critical infrastructure system and care must be taken when transmitting the electricity through the system to maintain the balance between consumption and production of electricity.

5.2.1. Results from the Questionnaire

The system operator has one business site other than the main office and is certified to ISO 9001 [2], ISO 14001 [11], and ISO 45001 [4] (previously OHSAS 18001). ISO/IEC 27001 [3] is in implementation phase. Written ISO management system policy documents exist where safety, security, and environmental risk is addressed. There is good knowledge of the legal environment. A formal risk management process is in place as a part of the ISO management system. This means that risk analysis and risk assessment are conducted. There is internal control, regular audits (internal and external), and a management review process. A formal risk analysis technique is used, implemented in a risk assessment software solution. ISO risk management guidelines are used. Both tangible and intangible assets are identified, and risk is related to assets. Threats to assets are identified and consequence of risk is assessed. Likelihood of risk is a factor in the assessment and risk is calculated. Risk management includes continuous improvements, systematic risk mitigation, assessment of risk control efficacy, cost analysis, documentation, and risk learning process. Risk criteria are set but residual risk is not assessed.

5.2.2. Results from the Interview

The head of system operation was interviewed. The interview revealed that the risk assessment process and risk analysis technique are mainly based on ISO/IEC 27001, which has not yet been fully implemented. Risk is analyzed and assessed in Excel templates and results from risk assessment, then stored in a central SQL database. Risk factors are identified, registered, and categorized in main categories and subcategories. Description of each risk factor, cause, and effect are registered. Likelihood and impact are estimated in numbers and then risk is calculated as a multiple of likelihood and impact, risk = (likelihood of risk) × (impact of risk). Both likelihood and impact are integers on a scale of 1–4. Risk tables in Excel and two-dimensional matrices with four different colors are used to show the severity of each risk factor. For each risk factor, there is one responsible person. Responsible departments are also registered, there can be more than one. A short description of an action plan to mitigate risk is registered with a follow-up plan, which is sometimes left unfilled. In some cases, if related to the finance department, a policy document is referenced with a note of measurements and risk criteria. A bottom-up risk assessment technique is used, and each department is responsible for assessing its own risk. All risk assessments are then collected into one risk library. Risk assessments are also conducted as part of project management. A risk overview with summary and statistics is provided through a management software interface.

Results from risk assessment and incidents that have happened reveal weaknesses in the system. To mitigate this risk, some parts of the system (old overhead lines) need to be renewed and some new lines must also be built in areas that are considered natural reserves. There have been disputes over how to build and maintain the system, which concern the choice of laying high voltage overhead lines and/or underground cables. Disputes with landowners who either do not want a power line across their land or want unacceptable compensation for their land cause delay. Further enquiry revealed that some existing risk factors have neither been registered nor assessed because it is not clear who is responsible. This applies to risk caused by hybrid threats and threats such as pandemics. Risks related to the lack of public policy support, international politics, and trends in technology (e.g., smart grid) that could affect the electricity transmission systems have not been identified.

5.2.3. Summarized Results from the Public Supply System

The public supply system is a critical infrastructure system. Risk analysis has revealed that electrical power security is insufficient in some places and breakdowns have led to power outages. The bottom-up risk analysis method has led to causal relationships between risk factors not being identified, the root cause has not been identified, and risk that does not clearly fall within one of the departments is not identified. Table 5 presents a summary of the results from the public supply system.

Table 5. Results from the public supply system.

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	Risk associated with stakeholders not always addressed	True
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Internal boundaries well defined but bottom-up risk assessment within departments has led to causality between risk factors not being identified	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	Hierarchical issues found	True
4	Resources available to support the RM system	Resource issues found	True
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Two-dimensional risk metrics does not capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk criteria sometimes unclear	True
8	Treatment of residual risk	Not every known risk is included in the risk assessment and treated therefore left as residual risk	True

5.3. Construction Company

The construction company (organization C in Table 2) constructs infrastructure facilities/products, operates them, and sells the product. The construction of each facility/project involves complex systems and equipment, as well as challenging construction work in often extreme conditions. The project analyzed in this study was divided into several contracts, some regarding construction work, some for equipment, and others for systems. The construction phase of the project analyzed in this study took five years and was finished in 2014. Altogether, the project took ten years including the preparation phase.

5.3.1. Results from the Questionnaire

The construction company has seven offices and is certified to ISO 9001 [2], ISO 14001 [11], ISO/IEC 27001 [3], and ISO 45001 [4]. Written ISO management system policy documents exist where risk regarding safety, security, and environment is addressed. There is good knowledge of the company's legal environment. A formal risk management process is in place as a part of the ISO management system. Risk analysis and risk assessment are conducted. There is internal control, regular internal and external audits, and a management review process. A formal risk analysis technique is used and implemented in Excel templates. ISO risk management guidelines are not used during the construction phase. Risk is assessed regarding threats/hazards, likelihood, and consequence. Risk management includes continuous improvements, systematic risk mitigation, cost analysis, documentation, and risk learning process. Efficacy of risk controls is not assessed. Risk criteria are partly set, and residual risk is not assessed in a formal way. Results from risk assessments are documented and used to learn from them.

5.3.2. Results from the Interview

The interview with the project risk manager revealed that the construction company takes a holistic approach to risk management and the company's risk manager is responsible for coordinating overall risk management tasks and maintaining ISO certifications. However, risk management in individual projects is led by a project risk manager. Both the risk manager of the construction project and the company risk manager were therefore interviewed. Two risk management teams were formed in the project, one in the preparation phase and another in the construction phase. In the preparation phase, a risk consultant led the work together with the project manager. The risk work in the construction phase was led by the project risk manager who worked closely with the project management team throughout the construction phase. Both teams included experts from the company and external consultants. Regular meetings were held, risk associated with the project identified, and actions taken to reduce the risk. The project risk manager kept records of all risk-related information during the project time. When the project was finished, a final report was compiled on project health, safety, and environmental issues where risk assessment and risk management were included. Despite complications during the project time, the project was considered an overall success. There were three measurable reasons for this: (a) the project time was met; (b) the cost estimate was met; (c) there were no serious injuries.

Although much energy and time was spent on the risk analysis, the project risk manager acknowledged that risk assessment is an underestimated part of work in projects like this one. Risk analysis is the basis for disciplined working procedures, to ensure that the right decisions are made at the right time, and to avoid mistakes. Often, the environmental impact is controversial and different interests need to be balanced. Stakeholders' views were included in the risk analysis. Contractors had to submit their own risk assessment for every work item before they could start the work. Risk factors were reviewed in risk meetings and compared with company own assessment. This way, both parties (construction company and contractor) could assess risk factors together. One reason for this is that the construction company (buyer) did not always know what equipment the contractor would be using. The aim of the meetings was to achieve the widest possible knowledge and understanding

of all risk related to the project. The meetings were sometimes big and difficult to manage, like brainstorming sessions. Discussions tended to drift, and much discipline was required. People got ideas and started discussing solutions while analyzing risk. This made the risk analysis difficult and complicated in practice. The goal was to somehow measure the outcome, results, and efficacy of the risk analysis, but no good way was found for such measurements. The ISO risk management guidelines were not used. The project risk manager considers the need for effective risk analysis methods in big construction projects both urgent and growing. The risk analysis of projects such as this one is often centered on operational risk in terms of finance. In the opinion of the project risk manager, simple risk models are good to get started and lay out the risk analysis. Then, it is necessary to dive deeper into different parts of the risk model. It can be disadvantageous for the construction company to tie things regarding construction projects too much with standards and regulation requirements. It can lead to overdesign and associated unnecessary costs.

The company's risk manager stated that there is one uniform risk assessment process within the whole company. He is responsible for the company risk register stored in a Microsoft SharePoint system. Other employees are responsible for assessing risk in Excel spreadsheets. The risk analysis is defined as identification of risk, registration, categorization, scoring, and comparison with risk criteria that are set in the beginning. This includes considering the business goals of the company, goals of risk management, and goals of every project. Scope and goal setting may differ. A matrix with colors and two scales, EBITDA, and company image is used to assess high-level company risk. Different scores are used for analyzing risk at other levels in the company. Moreover, the risk criteria differ depending on what is relevant to different departments and projects. The purpose of risk analysis is to: (a) ensure that the company achieves its goals; (b) provide an overview of risk; (c) ensure that the company does not suffer major setback/incidents that can have significant negative impact on its operations. In risk analysis, all risk factors are considered, regardless of likelihood and impact, but there needs to be a clear incentive and expectation of benefits before starting a risk analysis. Risk analysis is time consuming and often complicated. It is important that risk experts can communicate the risk information and make it easy for others to understand. The company risk manager believes that although the risk framework may be different within organizations, the technique/method and process of risk analysis can still be the same. Communication, information sharing, solutions, monitoring, and feedback may all be different.

In the opinion of the company's risk manager, risk analysis is too seldom a part of decision making. His view is that risk analysis must be built into company culture. It should be as natural to analyze risk as to calculate expected return on investment. This is often not the case; people tend to spend too little time on risk analysis when making decisions and simply assume they know everything there is to know. It is difficult to estimate the value of risk analysis and it can be challenging to explain and get people involved. It seems easier to analyze and assess risk where quantitative measurements are made, but qualitative evaluation is often necessary to reach full understanding. For many, it turns out to be difficult to choose a risk score or put a number on the risk. To be able to develop a risk culture within a company, it is important to review completed projects to learn from the experience, to give and get feedback, to improve and optimize the risk analysis process. If risk analysis is continuously applied as a business tool in daily use, it can aid in finding opportunities to improve the business. His opinion is that ISO standards can be helpful together with management system tools once risk has been identified. ISO 31000 [10] provides support and IEC 31010 [34] points out various techniques to analyze risk. The challenge, however, remains to identify the hazards, threats, and risk.

5.3.3. Summarized Results from the Construction Company

In this study, a single but complex construction project, lasting five years, was analyzed. Other parts of the organizations were not analyzed. Many contractors took part in the project. The company has been ISO certified to four management system standards

for decades and its risk management system is mature. Through many comprehensive construction projects, the company has developed a strong risk management culture. This has led to the company's risk management leaders being aware of the importance of risk analysis and risk management. Both the project risk manager and the company's risk manager believe that there are still opportunities to improve risk analysis and risk management within their company, e.g., with better coordination and integration into the company's overall management. Employees could be better educated and given better guidance in their work. ISO standards in general provide good support for risk management. The problematic question is: How much is a company willing to invest in the implementation and improvements of a risk management system? Key risk indicators need to be defined for indication of imminent risk. It is challenging to define what should be measured and monitored and it needs to be carefully done. Table 6 summarizes the results from the construction project. No issues were reported for benchmarks no. 5, 6, 7, and 8 in Table 6. This means that the hypothesis could not be verified.

Table 6. Results from the construction company.

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	No issues reported	Not verified
6	Risk assessment ability to capture risk evaluation	No issues reported	Not verified
7	Risk criteria setting in risk assessment	No issues reported	Not verified
8	Treatment of residual risk	No issues reported	Not verified

5.4. Manufacturing Company

The manufacturing company (organization D in Table 2) develops, produces, and sells medical devices. The subject in this study is a microcomputer-controlled (bionic) device. The questionnaire was answered by a project manager with help from a compliance manager and a quality assurance specialist.

5.4.1. Results from the Questionnaire

The company is listed on Nasdaq and has many subsidiaries and sites around the world. The design and production departments are certified to ISO 13485 [6] and ISO 14001 [11]. There is good knowledge of the company's legal environment. Written ISO management system policy documents exist where safety and environmental risk is addressed. A formal risk management system is in place that covers both the design department and the production department. The risk management system is supported by a proposal system and work request management system. Risk assessment and risk analysis is conducted in a formal way. Internal audits are conducted. There is a management review process in place. ISO 14971 [42] is used as risk management guidelines to medical devices together with IEC 62366-1 [43] guidelines for application of usability engineering to medical devices. They are both referenced in ISO 13485. Risk is assessed regarding hazards, likelihood or probability, and consequence. Risk management includes continuous improvements, risk mitigation, cost analysis, documentation, and a risk-learning process. The efficacy of risk controls is evaluated. Risk criteria are set, and residual risk is assessed. Results from risk assessments are documented and used to learn from them.

5.4.2. Results from the Interview

The project manager was interviewed. Experts working in the design department were also interviewed to fill in gaps. The project manager explained the complicated design and production processes of the microcomputer-controlled device. There are numerous things that need to be considered, e.g., the clinical needs, the patient safety, human error, and fulfillment of the user requirements. Development of new products follows a detailed product development process for new products where every step, milestone, and gate of the process is defined. Records regarding every product are kept for seven years after cessation of production. Medical devices are subject to extensive regulations to assure patient safety. The devices are divided into risk categories and classes, with different regulatory requirements. This classification is not internationally standardized, e.g., Europe, USA, and Canada all use different classification. Risk management is fundamental in demonstrating regulatory compliance for medical devices and it is a fundamental part of manufacturing processes in the medical device industry. Risk management for the product was based on a top-down Failure Modes Effects and Criticality Analysis (FMECA).

The guidelines for risk management for medical devices mostly come from ISO 14971 and IEC 62366-1, both referenced in ISO 13485. Neither ISO 13485 nor IEC 62366-1 refer to ISO 31000, but ISO 14971 does. ISO 14001, however, only refers to ISO 31000 for risk management guidelines. There is a difference in the core concepts and nomenclature of ISO 14971 and ISO 31000 that has caused confusion. Example 1: ISO 31000 defines "event" as "occurrence or a change of a particular set of circumstances" while ISO 14971 leaves event undefined. Example 2: "harm" is defined as "injury or damage to the health of people, or damage to property or the environment" while ISO 31000 leaves it undefined and unmentioned. Example 3: "risk" is defined as "effect of uncertainty on objectives" in ISO 31000, but "combination of the probability of occurrence of harm and the severity of that harm" in ISO 14971. Example 4: "risk management" is defined as "coordinated activities to direct and control an organization with regard to risk" in ISO 31000, but "systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling and monitoring risk" in ISO 14971.

In the opinion of the project manager, ISO 31000 offers a generic and abstract description of risk analysis but does not provide guidance on how to conduct it as such. ISO 14971 defines the risk analysis process for medical devices in four steps: (1) Intended use and reasonably foreseeable misuse; (2) identification of characteristics related to safety; (3) identification of hazards and hazardous situations; (4) risk estimation. The guidance ISO 14971 provides is, however, limited, e.g., "For each identified hazardous situation, the manufacturer shall estimate the associated risk(s) using available information or data. For hazardous situations for which the probability of the occurrence of harm cannot be estimated, the possible consequences shall be listed for use in risk evaluation and risk control". It still mentions several risk analysis methods in appendices, and the manufacturer is supposed to select the appropriate method. Guidance is given on risk identification in ISO 31000, but not mentioned in ISO 14971.

The manufacturing company used ISO standards to structure the risk management system. The risk analysis is embedded into every part of the product development phase. The risk analysis is a teamwork and the technique used has been developed within the company over time. Although it is based on ISO 14971, it also uses templates and classification systems specially designed and applicable to the production of medical devices. A risk ranking system is used for evaluation of suppliers. Process risk analysis is also done for the optimization of business processes and better utilization of raw material and components. The design of new bionic products is based on knowledge from previous products, but innovation is also an important factor. When analyzing risk, the focus is mainly on known hazards. The risk of a bionic device is related to (a) the mechanical structure and stability; (b) the bionic part that must not give electric shocks; and (c) software that does not fail. An event does not always have the same consequence. In case of the medical device in this study, the hazardous situations can vary, e.g., a person can fall on the ground or fall

in stairs, and so the severity level can also vary. The likelihood of an incident occurring is examined, followed by analysis of the incident severity. According to ISO 14971, the risk analysis process is a control process, i.e., the risk analyst shall identify what could happen that might form a hazard, then mitigating controls are selected. The manufacturer defines the acceptable risk and documents the process and communication of the results.

A Risk Priority Number (RPN) is calculated, based on severity of risk and likelihood of occurrence. It is challenging for the risk analysts to evaluate these factors. The RPN must meet predefined risk criteria for the development to continue. The key to an acceptable RPN is to neither overdesign nor overengineer safety because it is expensive. At regular intervals in the development process, there is an approval milestone or gate, and the product must pass certain gate criteria. At each gate, the result of the risk analysis is reviewed by an experienced person outside the risk analysis team but with good understanding and overview of the operation. If test results are good, it indicates that the product meets the requirements, and the severity factor should therefore decrease.

MS Word tables and Excel sheets are used for registering the risk analysis information which are then saved in a risk analysis file. An initial copy of the risk analysis file is saved when the product is launched, and a history log is kept for traceability. If an incident occurs after marketing the product, data are added to the risk analysis file and saved with a new version number. The update of the risk analysis can mean increase of risk because of defects in the medical device or decrease of risk because the use of the device is successful. Detection of hazards related to the use of the medical device is the most challenging thing in the risk analysis. The challenge is not only to detect foreseeable misuse, but furthermore to identify and analyze risk associated with such misuse.

5.4.3. Summarized Results from the Manufacturing Company

In this study, the development and production of only one medical device was analyzed, not the whole business. It has taken the company many years to optimize their manufacturing processes for bionic medical devices. Safety must be built into the design and risk must be managed throughout both design and production phases. The whole process is based on continuous and iterative risk analysis. Risk analysis experts have gone to great lengths in their risk analysis to develop safe products and meet the requirements of regulators. The risk control system has been a burden at times, where regulators demand ever-increasing formality and documentation. Now, a balance in the cost effectiveness and the regulatory compliance has been reached. Applying ISO standards is one way of meeting requirements from regulators, supervising authorities, and buyers (that are typically not end-users). Despite limited guidance on risk management in ISO standards and inconsistency in their definition of important risk terms, the ISO standards are essential for the business. Table 7 presents a summary of the results from the development and production of a medical device. No issues were reported for benchmarks no. 5, 6, and 8 in the table. This means that the hypothesis could not be verified.

Table 7. Results from the manufacturing company.

No.	Benchmark	Issues found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	No issues reported	Not verified
6	Risk assessment ability to capture risk evaluation	No issues reported	Not verified
7	Risk criteria setting in risk assessment	No issues found	False
8	Treatment of residual risk	No issues reported	Not verified

During the interview with the product manager, he raised the question: "Is the company perhaps doing too much on risk analysis and risk management?" He further stated that "risk management can easily go overboard, but the thin line to follow is to catch and deal with relevant risk without spending too many resources".

5.5. Software Company

The software company (organization E in Table 2) develops risk management software for an international client base, a modular software suite. It also provides hosting services and information technology consultancy. The software is a database hybrid (client-server and web-based) solution. It is mainly used by organizations for their business activities, but also for training and education at universities. The company is focused on innovation and collaboration with universities. It has received European project grants for the development of the software.

5.5.1. Results from the Questionnaire

The software company is listed on Nasdaq and has one subsidiary. All its business activities are certified to ISO/IEC 27001 [3]. There is good knowledge of the legal environment. Written information security policies exist, supported by other policies, e.g., access policy and teleworking policy. A formal risk management process is in place. Risk assessment and risk analysis is conducted, there is internal control, regular internal and external audits, and a management review process. Risk management software is used with a built-in risk analysis module. Risk is associated with both tangible and intangible assets. Threats to assets are identified, and consequence of risk is assessed. Likelihood of risk is a factor in the assessment and risk is calculated. Residual risk is assessed, and risk criteria are set. Risk is monitored, reviewed, and treated. Effectiveness of controls in terms of cost is not evaluated. Results from risk assessment are documented and used to learn from them.

5.5.2. Results from the Interview

The security manager of the software company explained that changes in ISO/IEC 27001 since 2005 have been confusing. The focus was on asset-based risk assessment methodology, but in the latest version, ISO/IEC 27001:2013, there is only mention of assets in Annex A. The referenced guidelines on risk management are ISO/IEC 27005 [44] and ISO 31000 [12]. There is a difference in the core concepts and nomenclature of ISO 31000 and ISO/IEC 27005. When it comes to risk analysis, ISO 31000 offers a generic and general risk management guidance but no guidance on how to conduct risk analysis as such. ISO/IEC 27005 offers limited guidance on how to conduct risk analysis, for example: (a) risk analysis depends on the criticality of assets; (b) it is based on assessed consequence and likelihood; (c) it can be done on a qualitative or a quantitative scale. The software company uses a combination of qualitative and quantitative risk assessment techniques built in a software solution.

The risk assessment is conducted in line with ISO/IEC 27001. It is based on assets, both tangible and intangible, and their properties in terms of value, confidentiality, integrity, and availability. Potential threats to assets and asset vulnerabilities are identified and assessed. Three risk calculations are made for every asset:

1. Inherent risk factor, the base security risk, is calculated for every asset based on four variables: the likelihood of threat, the impact of threat, the vulnerability of the asset towards the threat, and the value of the asset of which the threat is associated with. All four variables are evaluated on a scale between 1 and 5.

2. The second risk calculation is the current security risk. Risk is calculated with regard to implemented controls. A threat library is used in this calculation. Every threat is related to several controls from ISO/IEC 27001 which are meant to mitigate it. A calculation is made that considers, on the one hand, controls that are already implemented and, on the other hand, controls that have been defined as possible but

have not yet been implemented. This gives a risk factor that can be compared to the inherent risk factor to assess the benefits of the measures that have already been taken.

3. The third risk calculation is similar to the second risk calculation. It takes into consideration both implemented and future controls, i.e., controls which are being considered or have already been chosen to be implemented but have not yet been implemented. This calculation is made to evaluate the benefit of future controls.

Description of risk is written in a free-text fields, but history of risk changes is difficult to verify. The causal relationship of complex risk is not captured. Although risk criteria are set as numbers, the meaning of the numbers remains unclear. The efficacy and maturity of the controls (mostly taken from ISO/IEC 27001) are difficult to comprehend.

Through their international client base, mostly ISO certified organizations, the software company is aware of the limitations of ISO standards when applied to analyze and manage risk in challenging operations. The security manager pointed out that ISO standards provide little guidance on how to analyze and assess risk. Therefore, the company risk analysts have conducted their own studies based on state-of-the-art literature and collaborated with academic experts in the risk field. The aim has been to find methods to better capture and manage risk that arises from complex interactions and emergent behavior that is inherent in present-day socio-technical systems. Thus, systems theory methods (https://www.sciencedirect.com/topics/psychology/systems-theory, accessed on 9 March 2022) have been investigated and Systems-Theoretic Process Analysis (STPA) technique has been used [45,46]. In this way, risk factors have been identified that could not be identified with previous methods based on ISO/IEC standards. By the end of this case study, the software company already conducted its risk analysis in two ways, for comparison, in line with ISO standards and with the STPA technique. With STPA, risk and causal relationships were identified that had not been identified before, e.g., risk regarding company merger, lawbreaking of employees, breaches of confidentiality, industrial disputes, strikes, pandemic, and technology transitions.

5.5.3. Summarized Results from the Software Company

The results from the questionnaire are based on the certified ISO risk management system. The use of the systems theory method, STPA, has not yet been fully implemented in the risk analysis process. The use of risk management software ties the risk assessment, risk analysis, and the risk treatment to requirements and controls from ISO/IEC 27001. Risk calculations are performed in three ways to clarify and support risk management decisions. Various information is registered in free-text fields regarding asset properties, threats, likelihood, and vulnerabilities. This is to ensure that different parties within the company can assess the risk based on the same information and come to the same conclusion regarding risk. Despite the effort and the good awareness of the company's experts, it is their own assessment that various risk issues are present. Table 8 presents a summary of the results from the software company. It shows that only benchmarks no. 1 and 3 are without any issues.

Table 8. Results from the software company.

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	Fales
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Internal boundaries sometimes unclear	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	Lack of resources	True
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Limited ability to capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk setting unclear	True
8	Treatment of residual risk	Residual risk partly addressed	True

5.6. Pension Fund

The pension fund (organizations F in Table 2) has a governmental operating license and is subject to official supervision. The pension fund places great emphasis on risk analysis in its investments and the financial crisis in 2008 did not have a significant adverse effect on it. The fund did not have to reduce pension rights after the financial crisis. The investments are international, in bonds, equities, and mortgage loans for members. During the time of this study, the pension fund implemented a formal management system according to ISO management system standards. This was partly done to reinforce trust, but also to meet stricter regulatory requirements after the financial crisis.

5.6.1. Results from the Questionnaire

All the pension fund's business activities are certified to ISO/IEC 27001 [3] and ISO 9001 [2]. There is good knowledge of the legal environment. Written information security and quality policies exist. They are supported by other policy documents, e.g., risk policy and investment policy. A formal risk management process is in place. This means that risk assessment and risk analysis is conducted. There is internal control, regular audits (internal and external), and a management review process. Risk analysis is conducted, a formal risk analysis technique is used and recorded in Excel templates. Risk is associated with assets, both tangible and intangible. Threats to assets are identified, and consequence of risk is assessed. Likelihood of risk is a factor in the assessment and risk is calculated. Residual risk is assessed, and risk criteria are set. Risk is monitored, reviewed, and treated, efficacy of controls in terms of cost is not evaluated. Results from risk assessment are documented and used to learn from them.

5.6.2. Results from the Interview

The CEO of the pension fund was interviewed. He revealed that his participation in this study was a part of the pension fund's risk management reinforcement. All business procedures were reviewed during the time of this study with regard to requirements in ISO management system standards. The risk assessment process and risk analysis itself was also strengthened. External experts were hired to work with the management team and the board of directors. They submitted reports with forecasts and analyses. An advisory board including foreign experts was established.

A quarterly risk management report is prepared for the board based on the asset position. The report also includes analysis of financial changes, investment policy, currency development, economic forecast and prospects, breakdown of asset categories, return on assets over different periods of time (also categorized), Q/A on the asset portfolio, and overview of risk factors. The risk analysis, risk evaluation, and risk calculation are made in an Excel sheet that contains an overview of risk factors and risk calculations:

1. Basic risk score = ((impact of risk) × (likelihood of risk)) + (impact other than financial)
2. Quarterly risk score = (basic risk score) − ((effectiveness of mitigating control) × (basic risk score))
3. Previous quarterly risk score
4. Involvement of pension fund division
5. Responsible division
6. Description of risk factors
7. Possible consequences of risk
8. Description of mitigation controls
9. Objectives
10. Comments
11. Reference to a documented process

The risk score calculation is based on a two-dimensional risk matrix: x = impact of risk (on scale 1–7); y = likelihood of risk (on scale 1–4). Identified risk factors have remained the same over time.

At the end of this study, all work processes and procedures had been documented and linked to requirements in ISO standards ISO 9001 and ISO 27001. Standard requirements had also been analyzed in conjunction with departments. The development of risk analysis techniques continues and is not based on ISO standards. Awareness of societal and technological changes has reinforced managers' determination to analyze risk even better than before. Ways are being sought to further deepen the understanding of the risks associated with individual investment opportunities, especially those based on complex technologies.

5.6.3. Summarized Results from the Pension Fund

The pension fund's risk experts consider themselves well aware of financial and investment risk factors. This is confirmed by the fund's good performance in previous years. However, some risk factors have not been identified, e.g., risk associated with hybrid threats and world threats, such as pandemics, environmental threats, democratic threats, technology transition (e.g., blockchain), and international politics. Future international investments require risk to be carefully assessed and aligned with the investment policy. Not only the expected return on investment must be considered, but also requirements from members regarding sustainability, environmental impact, and ethics. Therefore, the risk analysis must not only be transparent, dynamic, and efficient, it must also be reliable and systematic in capturing new risk factors arising from present-day complex systems. Table 9 presents a summary of the results from the pension fund investments.

Table 9. Results from the pension fund.

No.	Benchmark	Issues found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Risk assessment ability to capture risk evaluation is limited	True
7	Risk criteria setting in risk assessment	Risk criteria unclear	True
8	Treatment of residual risk	Treatment of residual risk unclear and residual risk not always addressed	True

6. Discussion

The aim of this study was twofold, to develop a benchmarking model for risk management and to test it on six real-life and ISO-certified risk management systems.

6.1. First Aim: Development of a Benchmarking Model for Risk Management

The results of the study show that it can be difficult to assess the efficacy of risk management, even if the risk management system is ISO-certified. The certification is not a guarantee of being able to identify and assess all relevant risks in business operations. Methods and tools are needed to support evaluation of the efficacy and robustness of a risk management system. The two-step benchmarking model developed in this study can be used as a tool for this purpose and leaves opportunities for further development. The model uses an assessment template with a simple scoring system to verify and evaluate all main parts of a risk management systems. If the evaluation is positive and the risk management system proves to have all necessary parts in it, the next step is to dive deeper and assess the efficacy of individual parts of the system. Risk analysis and risk assessment are two of the most challenging parts for many organizations. These parts need to be examined

and evaluated regarding the ability to detect risk, often in complex systems. In this study, the participants assessed their own risk management systems through a questionnaire. The answers were supported by documents of various kind. After reviewing the answers and documents, interviews were conducted as audit meetings to verify all information provided. Step 2 in the benchmarking model was applied to capture qualitative data. The scoring was in the form of "risk issues found".

The study shows that it is important to build the benchmarks on risk science. Further research is needed to find out whether it is possible to develop a standardized scoring system based on risk science that serves as a good indicator of evaluation ability. There are also other aspects of risk management that need to be considered, for example, identification of risk leading indicators. Recent research has been conducted in this area [47]. The overall efficacy of the risk management system needs to be further examined. To handle complexity, robustness and resilience must also be addressed. More such factors need to be analyzed and ways found to measure and evaluate them.

Recent literature on risk management describes the importance of benchmarking models for improvements and quality assurance. The literature also describes various risk issues and challenges faced when managing risk in complex socio-technical systems. Several approaches to systems thinking have been proposed to understand such systems. These approaches may increase system and risk understanding but may still need to be supplemented with other approaches to adequately support risk management. Better modeling is advocated and qualitative modeling tools with description of systemic behavior are recommended for identification and evaluation of risk in complex systems. ISO 31000 neither addresses the importance of risk models nor describes how to go about creating such models.

6.2. Second Aim: Application of a Benchmarking Model for Evaluation of Real-Life ISO Risk Management Systems

The study shows that ISO standards can be applied in many ways in risk management systems, depending on the nature of the operation and the business needs. Evidence, results, and testimonials in this study confirm that risk management is increasingly important for business, and it is becoming an integrated part of a management system. This is in line with findings in a former study [8]. The study also shows that in all six cases examined, different approaches are taken to risk analysis and risk management. By applying the benchmarking model developed in this study, it was possible to find both risk issues and risk factors that had not previously been found.

The study provides evidence that despite the importance and good efforts, risk management and particularly the analysis of risk was not done satisfactorily in four out of six cases studied. Table 10 gives an overview of the risk issues found and in which organizations. The first two columns show the number and the name of the benchmarks. The third column shows the correspondence of the benchmarks to the three parts of the ISO 31000 risk management guidelines, i.e., principles, framework, and process. Columns 4–9 show the findings in the organizations' risk management system. The last column shows the frequency of risk issues found based on benchmarking. The "x" means that issues were found in the risk management system, " " (a blank) means that no issues were found, "(*)" means that risk issues could not be completely verified in this study. The last column shows the frequency of the risk issue (max 6). At the bottom of the table, the total number of risk issues found in every case is shown, max 8 risk issues in every organization A–F.

Table 10. Overview of the risk issues found and in which organizations.

No.	Benchmark	Corresponding to Risk Management (RM) in ISO 31000:2018	A—Public Health Service	B—Public Supply System	C—Construction Company	D—Manufacturing Company	E—Software Company	F—Pension Fund	Frequency of Risk Issues
1	Scope and outer boundaries of a RM system	Process: Scope, context, and criteria	x	x					**2**
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Process: Scope, context, and criteria	x	x			x		**3**
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	Principles: Structured, comprehensive, and dynamic Framework: Leadership and commitment Process: Risk assessment and treatment		x					**1**
4	Resources available to support the RM system	Framework: Leadership and commitment		x			x		**2**
5	Risk analysis ability to capture complex systems and business operations	Process: Risk assessment	x	x	n.v.	n.v.	x	x	**4**
6	Risk assessment ability to capture risk evaluation	Process: Risk assessment	x	x	n.v.		x	x	**4**
7	Risk criteria setting in risk assessment	Process: Risk assessment and treatment	x	x	n.v.	n.v.	x	x	**4**
8	Treatment of residual risk	Principles: Continual improvements Framework: Improvement Process: Risk assessment, treatment, monitoring, and review	x	x	n.v.	n.v.	x	x	**4**
	Total no. of risk issues found in RM system		**6**	**8**			**6**	**4**	**24**

"x" = risk issues found; " " = no risk issues found; "n.v." = could not be verified in this study.

This can be summarized as follows:

1. Scope and outer boundary issues were found in 2 out of 6 cases.
2. Interface issues were found in 3 out of 6 cases.
3. Hierarchical issues were found in 1 out of 6 cases.
4. Resource issues were found in 2 out of 6 cases.
5. Issues regarding risk analysis ability to capture complex systems and business operations were found in 4 out of 6 cases.
6. Issues regarding risk assessment ability to capture risk evaluation were found in 4 out of 6 cases.
7. Issues regarding setting of risk criteria were found in 4 out of 6 cases.
8. Issues regarding residual risk were found in 4 out of 6 cases.

Risk issues were identified in four out of six risk management systems. In the other two risk management systems, risk issues could not be completely verified (still marked as "No issues found"), which does not mean that risk issues did not exist at some point. Review of these findings with correspondence to the risk management description in ISO 31000:2018 (see Table 1) shows that there is weakness in the risk management principles, the framework,

and the process (see Figure 1). In view of the previous study, this is a clear indication of a lack of guidance on risk management and inconsistency in risk terminology in ISO standards, as demonstrated in [8].

Testimonials confirm that all the organizations are searching for better and more efficient risk analysis methods; a systematic method that provides better risk finding assurance. Common causes for risk factors are often not identified because of boarder and interface issues, complexity issues, and lack of overview. One of the reasons is the frequently used bottom-up approach in risk assessments, where different departments assess their own risk and then risk information is compiled into one risk register (risk library) without further risk analysis. Emergent behavior, time lags, and relevant control or feedback loops are not identified through the risk management approach in any of the cases.

The risk management systems of the construction company (organization C) and the manufacturing company (organization D) proved to be satisfactory for the two projects analyzed in this study, a construction of one infrastructure facility and the development of one medical device. Despite being very different, both management systems are mature and based on many years of experience. During the construction phase of the construction facility, no guidance from ISO standards was used. The manufacturer of medical devices developed a risk management system for the development of medical devices that uses ISO standards as a basis, but the risk analysis technique was developed by risk experts within the company, where experience and knowledge of the design and production of medical devices has a long history. The manufacturer of medical devices tries to capture risk related to user errors of the medical device. The software company (organization E) is the only case where systems theory has been applied, but only for a short time. It is still being tested but the company has managed to improve its identification and analysis of risk with help of the STPA technique [45,46].

Although it has not been specifically analyzed, it is obvious that the organizations in this study have invested significantly in their risk management systems. Once an accredited certification has been obtained, there is increased reputational and image risk involved in losing or giving up the certification. The support from top management is important, not only to establish the risk management system, but also to maintain it. It is understandable that people want to keep risk analysis as simple as possible. If a simple analysis has been done and it has been helpful, there is a reluctance to increase complexity, especially at increased cost. When is it necessary to take the next step? The decision is easier if a simpler and more cost-effective new method is found. Even then, regulatory requirements must be fulfilled.

During the time of the study (2014–2019) efforts to improve risk analysis were evident by the public supply system (organization B), the software company (organization E), and the pension fund (organization F). However, unsubstantiated methods are used, such as two-dimensional risk matrices, by all organizations except the software company. That company has been certified to ISO/IEC 27001 since 2004 and specialization in the risk field has driven knowledge and led to maturity of its risk management process which nevertheless has risk issues. All interviewees in this study noted that risk assessment, including risk analysis, has been a demanding and difficult task for them. Communicating results from risk assessments to either internal parties (e.g., board of directors) or external parties (e.g., governmental authorities), is also challenging. It was argued that especially third-party organizations (e.g., regulators, contractors, suppliers) did not always understand the effort associated with risk management. It was also argued that these parties lack an understanding of the complexity of risk management and the time and cost involved. This again increases risk.

7. Conclusions and Future Work

In this article, we have investigated how benchmarking theory can be combined with risk science and used to gain and improve understanding of the efficacy of a certified ISO

risk management systems in real business operations. It was hypothesized that although organizations have certified ISO risk management systems, certain flaws in risk management would be evident in practice, assuming that the representatives of the organizations in this study are describing the true situation in their organizations. The findings presented in Section 5 show that this is clearly the case in four out of six risk management systems, also shown in an overview in Table 10, cases A (with 6 types of risk issues), B (with 8 types of risk issues), E (with 6 types of risk issues), and F (with 4 types of risk issues). In the other two systems, C and E, this could not be verified, but risk issues could not be ruled out. Table 10 also reveals general weaknesses in risk analysis ability, risk assessment ability, setting of risk criteria, and treatment of residual risk. These are critical issues for managing risk in complex socio-technical systems.

In relation to the identification of hidden risk of organizations through the ISO standards-based risk management system, it was found that with the benchmarking model, more risk factors can be found without any significant changes to the risk identification and risk assessment processes. The benchmarking model in this study belongs to cross-sectoral type of benchmarking and it clearly helps identifying hidden risk, for example, risk associated with hybrid threats and world threats (such as pandemics), environmental threats, democratic threats, technology transition, and international politics. Although no defects of the model were observed during its use the model needs further refinement. It is adapted to ISO 31000, but the measurability of individual benchmarks needs further development in connection with use in diverse operations. For example, in this study, the measurement of risk criteria setting, and the treatment of residual risk consisted primarily in confirming that these factors were addressed. The way in which they were handled was examined but it was not possible to measure how effective the controls are. In order for this to be possible, the measurability needs to be investigated further and measurement techniques need to be developed.

All the organizations evaluated in this study have extensive experience in the use of ISO standards and showed both understanding and commitment in risk management. They all rely heavily on the risk management guidelines in ISO standards. They are all aware of weaknesses in their risk analysis techniques and acknowledge that it is partly due to inadequate guidance in the standards. With help of the benchmarking tool developed in this study it was possible to identify flaws in four out of six systems analyzed. Although no issues were reported in two out of six systems, the benchmark model identifies possible weaknesses that need to be further analyzed. This presents opportunities for improvement. It appears that all organizations are willing to change their approach to risk analysis if a better technique is found in the sense of uncovering risk that has previously been unidentified, being efficient, not too complicated, not manpower intensive, and not too expensive.

The limitation of this research lies in the data available, time required to analyze data, experts' knowledge needed to evaluate the data, an understanding of specific and complex systems, and changes that occur in perpetual systems over time. The weakness of the risk analysis conducted in this study lies in the measurability of both risk and efficacy of risk management. This is difficult to standardize, and every organization must find an appropriate risk analysis technique where causal relationship of risk factors, risk criteria, risk acceptance, and residual risk can be made understandable and measurable. It would be of great value if ISO standards contained better guidance to help and support their users in this continuous process.

The findings, however, show that there is a strong reason to further investigate the measurability of effectiveness in operation risk management systems. This is a subject for future work. The practical implications of the study are of value for company managers, risk analysts, and those who develop standards, e.g., ISO. This study also contributes to benchmarking theory and highlights the challenging task to measure qualitative risk factors, being able to define measurable risk factors and having the right measure to assess the risk. It reveals the importance of building risk management systems in organizations on a risk

science foundation. As future work, the authors plan to further develop the benchmarking model based on recent risk science literature and to test the model in more organizations.

Societies are undergoing a huge change, often referred to as the fourth industrial revolution (https://www.weforum.org/focus/fourth-industrial-revolution, accessed on 9 March 2022). This means increasing automation and a revolution in the use of digital solutions by people and organizations. This development is intertwined with, e.g., biotechnology, environmental issues, and sustainability requirements. This change can provide great benefits to societies. However, these developments bring new and previously unknown risks and threats, e.g., to nature, democracy, humanity, and health. According to the Global Risks Report 2021 and 2022, published by the World Economic Forum, the COVID-19 pandemic has accelerated this revolutionary change [48,49]. Such risks are not a private business matter, such as a quality of a product or a service, and cannot be treated as a strategic variable within an organization (like quality). Therefore, behind the decision of an organization to take risk, there should be consideration of many aspects of potential positive or negative consequences.

For the forthcoming changes to be successful and beneficial for societies and businesses, a constructive risk culture must be created within businesses, such that important decision making is well thought through and supported by risk analysis. Solid risk analysis must become inevitable in all management and decision making. ISO standards are an important foundation to build on. However, if the risk management guidelines of ISO standards are inappropriate, there is a high risk that they will not achieve their aim to support and strengthen businesses. Previous research [8] confirms the lack of guidance in ISO standards in risk analysis, especially regarding risk in complex socio-technical systems. To redress this, ISO should review its business strategy and base the guidelines more on risk science, for example, through active collaboration with organizations like the Society for Risk Analysis (https://www.sra.org/, accessed on 9 March 2022).

Author Contributions: S.H.B. conducted the research, led the study, and arranged the paper in the present conceptualization form. P.J. supervised the research and contributed to the writing and review. S.E.T., I.M.D. and R.J.d.B. contributed to writing, review, and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki and approved in accordance with the requirements of the Institutional Review Department of Reykjavik University (RU-DoE-Review-Board-Oct 2021, 28 October 2021).

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the six organizations and their representatives for participating in this study. Thanks for sharing their hazard and risk analysis and for the inspiring risk-related discussions. Their interest, integrity, and support made this study an informative and pleasant journey that lasted five years. Thanks also to the reviewers of this article and their valuable comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. COPOLCO. 2021. Available online: https://www.iso.org/sites/ConsumersStandards/1_standards.html (accessed on 15 February 2021).
2. *ISO 9001:2015*; Quality Management Systems—Requirements. ISO: Geneva, Switzerland, 2015.
3. *ISO/IEC 27001:2013*; Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO: Geneva, Switzerland, 2013.
4. *ISO 45001:2018*; Occupational Health and Safety Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/37/63787.html (accessed on 9 March 2022).

5. *ISO 22000:2018*; Food Safety Management Systems—Requirements for any Organization in the Food Chain. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/54/65464.html (accessed on 14 July 2020).
6. *ISO 13485:2016*; Medical Devices—Quality Management Systems—Requirements for Regulatory Purposes. ISO: Geneva, Switzerland, 2016.
7. *ISO 37001:2016*; Anti-Bribery Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2016. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/50/65034.html (accessed on 9 March 2022).
8. Björnsdóttir, S.H.; Jensson, P.; de Boer, R.J.; Thorsteinsson, S.E. The Importance of Risk Management: What is Missing in ISO Standards? *Risk Anal.* **2021**. [CrossRef] [PubMed]
9. International Accreditation Forum, Inc. International Accreditation Forum—IAF. *Find Members, Publications & Resources*. 13 July 2020. Available online: https://www.iaf.nu/ (accessed on 7 September 2020).
10. ISO—Management System Standards List. Available online: https://www.iso.org/management-system-standards-list.html (accessed on 9 July 2020).
11. *ISO 14001:2015*; Environmental Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2015.
12. *ISO 31000:2018*; Risk Management—Principles and Guidelines. ISO: Geneva, Switzerland, 2018.
13. *ISO 19011:2018*; Guidelines for Auditing Management Systems. IEC: Geneva, Switzerland, 2018. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/00/70017.html (accessed on 20 July 2020).
14. Talapatra, S.; Uddin, M.K.; Rahman, M.H. Development of an Implementation Framework for Integrated Management System Based on the Philosophy of Total Quality Management. *Am. J. Ind. Bus. Manag.* **2018**, *8*, 6. [CrossRef]
15. Talapatra, S.; Uddin, M.K. Prioritizing the barriers of TQM implementation from the perspective of garment sector in developing countries. *Benchmarking Int. J.* **2019**, *26*, 2205–2224. [CrossRef]
16. Franceschini, F.; Galetto, M.; Cecconi, P. A worldwide analysis of ISO 9000 standard diffusion: Considerations and future development. *Benchmarking Int. J.* **2006**, *13*, 523–541. [CrossRef]
17. Herbst, N.; Bauer, A.; Kounev, S.; Oikonomou, G.; Eyk, E.V.; Kousiouris, G.; Evangelinou, A.; Krebs, R.; Brecht, T.; Abad, C.L.; et al. Quantifying Cloud Performance and Dependability: Taxonomy, Metric Design, and Emerging Challenges. *ACM Trans. Model. Perform. Eval. Comput. Syst.* **2018**, *3*, 1–36. [CrossRef]
18. Kounev, S.; Lange, K.-D.; von Kistowski, J. *Systems Benchmarking: For Scientists and Engineers*; Springer International Publishing: Cham, Switzerland, 2020. [CrossRef]
19. Olawumi, T.O.; Chan, D.W.M. Development of a benchmarking model for BIM implementation in developing countries. *Benchmarking Int. J.* **2019**, *26*, 1210–1232. [CrossRef]
20. Van der Voordt, T.J.M.; Jensen, P.A. Measurement and benchmarking of workplace performance: Key issues in value adding management. *J. Corp. Real Estate* **2018**, *20*, 177–195. [CrossRef]
21. Staiger, R.D.; Schwandt, H.; Puhan, M.A.; Clavien, P.-A. Improving surgical outcomes through benchmarking. *Br. J. Surg.* **2019**, *106*, 59–64. [CrossRef]
22. Hartono, E.O.; Abdullah, D. HFLTS-DEA Model for Benchmarking Qualitative Data. *Int. J. Adv. Soft Compu. Appl.* **2019**, *11*, 109–131.
23. Mangla, S.K.; Luthra, S.; Jakhar, S. Benchmarking the risk assessment in green supply chain using fuzzy approach to FMEA: Insights from an Indian case study. *Benchmarking Int. J.* **2018**, *25*, 2660–2687. [CrossRef]
24. Hoffmann, P.; Schiele, H.; Krabbendam, K. Uncertainty, supply risk management and their impact on performance. *J. Purch. Supply Manag.* **2013**, *19*, 199–211. [CrossRef]
25. Björklund, M. Benchmarking tool for improved corporate social responsibility in purchasing. *Benchmarking Int. J.* **2010**, *17*, 340–362. [CrossRef]
26. Moriarty, J.P.; Smallman, C. En route to a theory of benchmarking. *Benchmarking Int. J.* **2009**, *16*, 484–503. [CrossRef]
27. MacGillivray, B.H.; Sharp, J.V.; Strutt, J.E.; Hamilton, P.D.; Pollard, S.J.T. Benchmarking Risk Management Within the International Water Utility Sector. Part II: A Survey of Eight Water Utilities. *J. Risk Res.* **2007**, *10*, 105–123. [CrossRef]
28. Talapatra, S.; Uddin, M.K.; Antony, J.; Gupta, S.; Cudney, E.A. An empirical study to investigate the effects of critical factors on TQM implementation in the garment industry in Bangladesh. *Int. J. Qual. Reliab. Manag.* **2019**, *37*, 1209–1232. [CrossRef]
29. Talapatra, S.; Uddin, K. Understanding the difficulties of implementing TQM in garment sector: A case study of some RMG industries in Bangladesh. In Proceedings of the International Conference on Mechanical, Industrial and Materials Engineering 2017 (ICMIME2017), Rajshahi, Bangladesh, 28–30 December 2017; p. 6. Available online: http://icmime-ruet.ac.bd/2017/DIR/Contents/Technical%20Papers/Industrial%20Engineering/IE-243.pdf (accessed on 1 November 2021).
30. Talapatra, S.; Uddin, K. *Some Obstacles that Affect the TQM Implementation in Bangladeshi RMG Sector: An Empirical Study*; IEOM Society International: Bandung, Indonesia, 2018; p. 13. Available online: http://ieomsociety.org/ieom2018/papers/401.pdf (accessed on 9 March 2022).
31. Aven, T.; Zio, E. Foundational Issues in Risk Assessment and Risk Management. *Risk Anal.* **2014**, *34*, 1164–1172. [CrossRef]
32. Klinke, A.; Renn, O. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Anal.* **2002**, *22*, 1071–1094. [CrossRef]
33. Cox, L.A. What's Wrong with Risk Matrices? *Risk Anal.* **2008**, *28*, 497–512. [CrossRef]

34. *IEC 31010:2019*; Risk management—Risk assessment techniques. IEC: Geneva, Switzerland, 2019.
35. Aven, T. Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. *Reliab. Eng. Syst. Saf.* **2017**, *167*, 42–48. [CrossRef]
36. Fellows, R.; Liu, A.M.M. Managing organizational interfaces in engineering construction projects: Addressing fragmentation and boundary issues across multiple interfaces. *Constr. Manag. Econ.* **2012**, *30*, 653–671. [CrossRef]
37. Mikes, A. From counting risk to making risk count: Boundary-work in risk management. *Account. Organ. Soc.* **2011**, *36*, 226–245. [CrossRef]
38. Zerjav, V. Design boundary dynamics in infrastructure projects: Issues of resource allocation, path dependency and problem-solving. *Int. J. Proj. Manag.* **2015**, *33*, 1768–1779. [CrossRef]
39. Lathrop, J.; Ezell, B. A systems approach to risk analysis validation for risk management. *Saf. Sci.* **2017**, *99*, 187–195. [CrossRef]
40. Blood Transfusion Guide—EDQM Publications | EDQM—European Directorate for the Quality of Medicines. 2020. Available online: https://www.edqm.eu/en/blood-guide (accessed on 29 April 2021).
41. WHO Action Framework to Advance Universal Access to Safe, Effective and Quality Assured Blood Products. 2020. Available online: https://www.who.int/publications-detail-redirect/action-framework-to-advance-uas-bloodprods-978-92-4-000038-4 (accessed on 29 April 2021).
42. *ISO 14971:2019*; Medical Devices—Application of Risk Management to Medical Devices. ISO: Geneva, Switzerland, 2019. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html (accessed on 9 March 2022).
43. *IEC 62366-1:2015*; Medical Devices—Part 1: Application of Usability Engineering to Medical Devices. IEC: Geneva, Switzerland, 2015.
44. *ISO/IEC 27005:2018*; Information Technology—Security Techniques—Information Security Risk Management. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html (accessed on 13 July 2020).
45. Leveson, N. A new accident model for engineering safer systems. *Saf. Sci.* **2004**, *42*, 237–270. [CrossRef]
46. Leveson, N.G. Engineering a Safer World. 2011. Available online: https://mitpress.mit.edu/books/engineering-safer-world (accessed on 3 July 2018).
47. Leveson, N. A systems approach to risk management through leading safety indicators. *Reliab. Eng. Syst. Saf.* **2015**, *136*, 17–34. [CrossRef]
48. The Global Risks Report 2021. *The World Economic Forum*. 2021. Available online: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (accessed on 12 April 2021).
49. The Global Risks Report 2022. *The World Economic Forum*. 2022. Available online: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (accessed on 9 March 2022).