electronics

MDPI

Review

A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection

Hamed Taherdoost

Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B 1V9, Canada; hamed.taherdoost@ucanwest.ca or hamed.taherdoost@gmail.com or hamed@hamta.org; Tel.: +1-236-889-5359

Abstract: Businesses are bombarded with great deals of risks, vulnerabilities, and unforeseen business interruptions in their lifetime, which negatively affect their productivity and sustainability within the market. Such risks require a risk management system to identify risks and risk factors and propose approaches to eliminate or reduce them. Risk management involves highly structured practices that should be implemented within an organization, including organizational planning documents. Continuity planning and fraud detection policy development are among the many critically important practices conducted through risk management that aim to mitigate risk factors, their vulnerability, and their impact. Information systems play a pivotal role in any organization by providing many benefits, such as reducing human errors and associated risks owing to the employment of sophisticated algorithms. Both the development and establishment of an information system within an organization contributes to mitigating business-related risks and also creates new types of risks associated with its establishment. Businesses must prepare for, react to, and recover from unprecedented threats that might emerge in the years or decades that follow. This paper provides a comprehensive narrative review of risk management in information systems coupled with its application in fraud detection and continuity planning.

Keywords: information systems; risk management; risk assessment; fraud detection; risk control; risk policy; continuity planning

Citation: Taherdoost, H. A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection. *Electronics* **2021**, *10*, 3065. https://doi.org/10.3390/electronics10243065

Academic Editor: Shinichi Yamagiwa

Received: 12 November 2021
Accepted: 7 December 2021
Published: 9 December 2021

1. Introduction

As different businesses are changing to become more complex, information and data processing plays an important role in the effective operation of different departments within an organization. Data processing, in an attempt to gain well-organized information, is a substantially time-consuming effort as great and growing volumes of data require further processing. However, the advances in computer-based systems have largely contributed to the development of systems to streamline the specific practices associated with data processing, specifically collecting, storing, processing, analyzing data, and also extracting and disseminating information for particular purposes. Such systems are referred to as information systems (IS) which play important roles within an organization aiming to increase the effectiveness of managerial decision making [1].

An information system can benefit an organization in many ways, mainly for upper-end decision-making goals. For instance, within hospitals and healthcare systems, increasing patient involvement and well-being while improving service quality and lowering costs are among the major benefits of a healthcare information system [2]. Alongside the general purposes of an information system, its major advantages within an organization can be outlined as accessing a great deal of data, pursuing effective decisions in an automated manner, reducing human errors due to the employment of complex algorithms, and helping to develop new approaches in gaining revenue and an increase in customers. A great example of the importance of an information system within an organization is the Amazon

E-commerce company [3]. A specialized integrated information system in Amazon has largely contributed to obtaining a competitive advantage reflected from the enhanced and efficient collection, storage, and analysis of data. One of the noteworthy advantages of Amazon's integrated information system is the decentralized decision-making process which largely contributes to reduced managerial diseconomies [1,3,4].

However, aside from the wide range of advantages and success factors that the information system suggests, the establishment of such a system in an organization may bring about several challenges limiting its implementation. Several challenges according to information systems can be listed as follows: (i) the constant changing of technology day by day requiring updated users to be in the learning mode, (ii) security issues related to vendors, banking, and distributing the essential data, intellectual properties, and records of the company, (iii) the inefficient establishment of an information system due to the high costs and expenses associated with it. These challenges coupled with long-listed ones can bring about potential risks substantially affecting an organization's effective performance. The sheer number of risks and risk factors associated with the business and information system establishes a driving force towards developing an organizing framework to manage and further respond to them. Accordingly, risk management practices are widely developed in order to mitigate the associated risk effects and increase the efficient performance of information systems within an organization.

Hence, due to the broad range of advantages risk management provides, it plays an important role in the appropriate functioning of different businesses and organizations. The associated importance is majorly due to the fact that as the different organizations are moving within the information systems area, the risk management considerations become highly essential to eliminate or mitigate the aforementioned risks associated with the incorporation of information systems within an organization. However, risk management represents a broad area of science, and the expertise gathered over time grows more sophisticated and interdisciplinary [5]. Accordingly, a lack of a comprehensive understanding has significantly failed to provide researchers and active practitioners with the big picture of risk management regarding information systems. In this review paper, we aim to present a comprehensive overview regarding the role of risk management within information systems to provide advantageous information for both researchers in the field and industry decision-makers.

In this article, we have attempted to provide a narrative literature review regarding the concept of risk management within the area of information systems. A narrative literature review summarizes several sources of research from which conclusions may be derived as part of a holistic interpretation informed by the reviewer's own experiences, theories, and models [6]. Throughout this manuscript, an overview of the importance of decision making within information systems and the associated conceptualization of risk, risk factors, and risk management are given. Risk management challenges are studied from a variety of scientific perspectives (e.g., social sciences, psychology, computer science, etc.). Risk management's interdisciplinary and multidimensional characteristics make it challenging to spot leading research patterns. However, we have tried to provide a specific framework to implement risk management with information systems. Since various organizations are highly threatened by uncertain and unpredicted business interruptions and associated challenges, unplanned events can bring about serious and catastrophic effects on a business. Accordingly, we have dedicated subsequent sections to provide an overview of the factors required to maintain business continuity in uncertain situations and to provide associations in relation to information systems. In the last section, an overview of fraud and fraud management has been presented since many organizations are highly threatened by associated risks, specifically those related to third party inclusion. Every vendor or partner carries the risk of a security vulnerability. Even if a business follows the greatest cybersecurity practices, a third party might compromise its data, customers, or reputation. Hence, it is of high importance to cover the concept of managing third party-associated risks and fraud control. It is also important to mention that, in this

manuscript, the term fraud is referred to the one which applies to information systems and their associated areas.

2. Research Methodology

Literature reviews, unlike original research papers, do not provide fresh discoveries based on data; rather, they aim to analyze what has been published in the primary research on a certain issue. As a result, the primary goal of this literature review is to provide the readers with a better understanding of risk, risk management, and its manifestation in fraud and continuity planning. The literature search for this review was conducted along the lines of narrative review searches, which mainly depended on four substantial electronic databases, including Google Scholar, ScienceDirect, Scopus, and ResearchGate. Articles used throughout this narrative review were selected based on search terms of risk, risk factors, risk management, information risk management, decision making, continuity planning, risk control policy, and information system fraud, alone or in combination. All the articles that were retrieved in their entirety had their reference lists scanned. Duplicates were removed from the search results once they were pooled. All paper titles and abstracts were scrutinized. The full texts of possibly relevant papers were examined, and the reference lists of those publications were searched for other related articles. Accordingly, any research that dealt with risk management, continuity planning, and fraud in English met the criteria for inclusion. Each component of this narrative evaluation was based on information from the selected papers, which was summarized and utilized.

3. Decision-Making

Information plays the most substantial role in decision-making within organizations. Accordingly, information systems were developed to provide the required information in a well-organized manner so that managers can engage in effective decision-making processes. The interrelation of information systems and decision-making is a key concern in information system science. Effective decision-making is largely reflected by the reduction of risks threatening the business and by a guarantee of the correctness of the provided information-key components that are ensured via information systems. As a result, software-based systems were developed specifically intended to compile raw data to obtain helpful information in line with solving problems and mitigating risk, which is specifically regarded as the decision support systems. However, in establishing and developing such information systems, it is required to understand the decision-making process against the risks threatening the business. In this concept, risk-related decisions are generally defined as the decisions that reduce or increase the danger of a significant accident in a sociotechnical system [7].

Nowadays, risk analysis is largely regarded as a scientific area of study, which was sometimes a debating issue. Risk science, which is mostly involved with (i) the knowledge concerning the risk-associated processes and events, and (ii) developing theories, methodologies, frameworks, and models for understanding and assessing risk, is relied upon as a strong basis for decision-making concerning risks [8,9]. Accordingly, a model that approximates the flow of information in the process through which science is accounted as a base for decision-making, providing the scientific nature of risk analysis, is illustrated in Figure 1 [9]. It clearly shows the links between facts and values in risk decision-making [9,10].

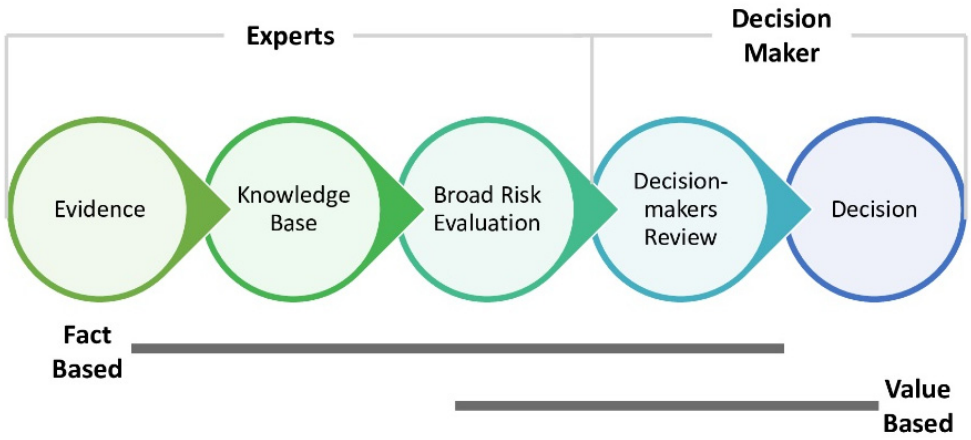

Figure 1. The links between facts and values in risk decision-making [9].

First, the analyses and examinations provide sets of data and information which are accounted for as evidence through the process. This provided evidence contributes to creating a knowledge base that is specifically "the objectified and well-organized information that contributes to drawing conclusions". After an evidence and knowledge base is created, it is necessary to add evaluation and assessment coupled with a primary judgment regarding the risks of the case under investigation, which is highly dependent on the scientific issues, so that related experts can be responsible for accomplishing it. In addition, the associated knowledge base evaluation should involve the decision makers' values and also delineate a clear border between the scientific burden of proof and the practical burden of proof. However, these primary judgments are not enough to directly make final decisions. Accordingly, the decision-makers are required to pursue information beyond the knowledge-based risk assessment, combining the obtained risk information with that of other resources, which clearly, along with scientific issues, covers further value-related considerations. Hence, the decision relies on a mixture of both factual and value-based considerations. Adding to this simplified model, there should be several other communications between different components, including questions provided to scientists by decision-makers [10,11].

Generally, the development and establishment of an information system within an organization contributes to mitigating the business-related risks and creates new risks associated with its own establishment. The existence of such risks requires a system that can clearly identify risks and propose approaches in eliminating or reducing them, which is known as a risk management system. Before discussing the main and underlying principles of risk management, a clear understanding of the risk and its associated terms should be established [12,13].

4. Risk

4.1. Risk Conceptualization

Every scientific area is highly dependent on clear, well-defined, and broadly accepted terms and definitions. The risk management field is no exception. Accordingly, there have been numerous attempts to provide a generally accepted definition for the term "risk"; however, there is still specific dissatisfaction with the proposed definitions [9,14]. In this regard, Lawrence in 1976 defined risk as "the measure of probability and the weight of undesired consequences" [15]. In 1989 risk was defined by Kaplan and Garrick as "the triplet (si, pi, ci), where si is the set of scenarios, pi is the likelihood of that scenario, and ci is the consequence of the scenario, i = 1, 2, . . . , N" [16]. In a similar manner, the United States Department of Defense describes risk as "the expression of influence and possibility of an accident in the sense of the severity of the potential accident and the probability of the event" [17]. Furthermore, in 2009, Aven and Renn [18] referred to the term risk as "the uncertainty about and severity of the events and consequences (or outcomes) of an

activity with respect to something that humans value". These varied definitions proposed in the literature can be categorized into three classes through which risk is described by (a) unpredictability and anticipated values, (b) by events/consequences, as well as ambiguity, and (c) in accordance to objectives. There have been various attempts to provide a generally accepted and unified definition of risk, but none have been widely agreed upon. This failure in establishing a unified viewpoint can be majorly attributed to several factors including: first, the fact that risk requires much more development and research; second, getting to a generally agreed-upon definition is abrogated since the literature research is now focused on creating new horizons and ideas; and third, the associated standardizing organization are not capable of proposing unified definitions that are agreed upon in the scientific community [19]. Although the proposed definitions may vary in some specific components, they all have a particular key point in common; all proposed definitions agree on focusing on the possible adverse or catastrophic consequences of a particular activity with respect to a set of specific human values. Accordingly, the proposed definitions almost differ in the way they measure negative consequences, defined as the possibility of occurrence, uncertainty, potential etc. Not surprisingly, the terms "risk" and "uncertainty" are being interchangeably used in different communities, while scientifically speaking, there are subtle differences between these two terms. Here in this manuscript, we simply define the term "risk" as the "cumulative effect of the probability of uncertain occurrences that may positively or negatively affect project objectives". In reality, its meaning is a topic of concern in all areas. In contrast, uncertainty refers to dealing with the points through which the probability is entirely unrecognized or unable to be recognized. In other words, risk considers the relative level of the occurrence probability of a specific event, while uncertainty is defined by the probability of being fully unknown [20,21].

Inherently, three main elements can be attributed to any risk, including the event, the probability, and the impact (or severity). The event is attributed to the description of any risk as it may come about. Without an explicit definition of the event, specifying and characterizing the probability and the severity is considerably complicated. To exemplify, the associated probability and impact characteristics of the prevalence of the COVID-19 virus differ among children and old people. Accordingly, the event description is a key step in assessing risks, and it should be determined in full sentences. This might be difficult in some specific fields such as cybersecurity, where in comparison to other fields, the risk is less tangible, and for some users, security is not a primary issue [22,23]. After fully defining the event, the potential severity of the risk's impact should be characterized so one can specify the degree to which the objective is affected. The assessment of the risk probability is highly dependent on the risk severity. The statistical and probability theories and methodologies utilized in this step are highly dependent on any existent historical record regarding the uniquely defined projects. This may bring about specific challenges since no or minimal records may exist [21].

4.2. Information Systems Risk

Definitions of information systems risk similarly cover a wide area but have main components in common, just as the general definitions of risk. Among the various proposed definitions for information system risk, are those attributed to the risks correlated with information development and data security. However, in a simplified manner, we can define information system risk as to the cumulative effect of the uncertainty of objectives and their impacts, resulting from the poor quality of information, on the intelligent information system involved in achieving those objectives [24,25].

As mentioned, the information system risks can be attributed to their development and security. In other words, risks can be correlated with the implementation period or post-implementation of the information system within an organization. Generally, the impacts of risk events associated with the implementation and development of information systems are limited to monetary issues such as loss of invested resources, while the impacts associated with the post-development of information systems can be much more striking

since the operational information systems are strictly involved within the environment of the business that they are supporting. For instance, during June 2007, a two-hour-last system shutdown happened in a mission-critical system in United Airlines, which made the organization cancel more than 20 flights and brought about $10 million losses for the company. Risks associated with the post-development of information systems within an organization are specifically known as the operational risk, which according to the Basel Committee on Banking Supervision, is referred to as "the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events" [25–27].

The reason associated with negative outcomes of information system-related risks in both phases of implementation and post-implementation has been attributed to the influence of risk components and risk factors. Generally, there have been different components reported to be associated with information systems majorly categorized as project risks, including the financial, temporal, or quality constraints, security risks associated with established systems within an organization, functionality risks comprising technical and technological constraints, and political risks impacting the associated relationships in a specified business. The IS-associated risks can be revealed in one or several fields, which are amplified with specific risk factors. Risk factors are attributed to particular factors in which their occurrence or presence increases the probability of the occurrence of negative outcomes associated with a risk event. There are many risk factors detected and discussed in different investigations within various fields (e.g., in healthcare systems [28,29]). These can be classified into ten groups, including: (1) top management support; (2) processes management; (3) involvement of end-users; (4) IS developing management; (5) requirement analysis; (6) project plan; (7) project management, monitoring, and evaluation; (8) team project management; (9) team experience management; and (10) team communication management. Although these factors and components are classified as mentioned, there is a great extent of overlap among them. In fact, they are not independent, and there is a high interrelationship among them. Understanding the associated relationship between such factors can contribute to better risk management [27].

Along with focusing on information systems risks, it should be considered that such systems are just an element within the manager's business environment, and most of the risks that occur might have originated from an external source and are not inherently dedicated to the system. Accordingly, a work system framework should exist in an organization to account for these factors, organizing them, specifying their interrelationship, and responding to them.

5. Principles and Aims of Risk Management

Companies that employ effective risk management must handle a wide range of risks in a coordinated manner, instead of conventional risk management, which manages each risk separately [30]. Risk is inherently characterized by three specific principles of (i) being partially unknown, (ii) being variable over a time period, and (iii) being altered by human actions [24,31]. These characteristics of risk are considered as driving forces that establish and develop specific methodologies, frameworks, and principles through which managers are compelled to dedicate focused resources to managing project risks and to establish organizational infrastructure aiming to achieve specific targets, including:

- Delineating which risks are financially, energetically, and temporally worth an investment;
- Isolating and optimizing risks;
- Eliminating destructive risks and improving progressive risks;
- Developing alternative sets of action spaces;
- Reserving time and money to withstand the threats that cannot be mitigated;
- Ensuring no breach over the organizational risk boundaries.

Through the passage of time, various structures and definitions (e.g., Octave Allegro at Education Institution methodology [32]) have been used for the same concepts in risk management, which has been accounted as a source of continuing confusion. However, here

we are discussing one of the most important structures attributed to risk management which is indeed in line with most of the risk management textbooks, as shown in Figure 2 [9,24,31].

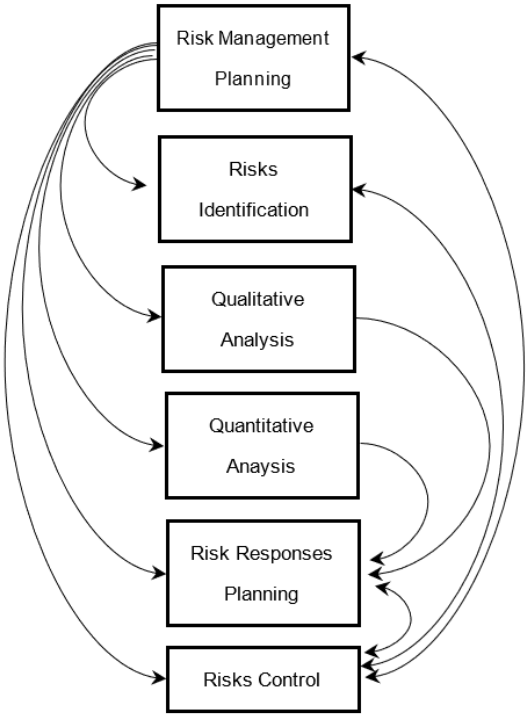

Figure 2. Main structures attributed to risk management [31].

5.1. Risk Management Planning

The first step in this process is risk management planning, in which the main goals and criteria of the risk management actions are specified. A series of strict plans are responsible for guiding the projects, through which, the projects are provided with rationale processes to aid in their execution. The risk management plan should also be part of a guiding plan which would provide the latest result or status of the risk management planning process. However, in comparison to other plans and struggles in the field, risk management plans have not been well-established in a specific content or format by which managers can simply establish well-organized frameworks and documents. Hence, different organizations pursue different ways of approaching the content of risk management plans. For example, the content of a risk management plan may include a complete description and project summary, risk environment, approach to risk management, application issues and problems, risk governance, process approaches, etc.

Describing the risk environment is an undeniable part of each risk management plan. In any kind of major and minor project, there is a risk environment through which the threats and opportunities present, and the ways of handling them should be specified. In this scheme, risk management planning is the struggle to bring the risk policies, procedures of the organization, and practices into a consistent whole by which the nature of project risk is addressed [9,24,25].

5.2. Identifying Risk

Risk identification is an essential step in every risk management process. This refers to an organized approach to find real risks and identify explicit situations and events that may impact specified aims and activities associated with the project. Risk assessment and risk management can only be performed after providing a clear vision of the risks, hazards, and opportunities. This is accomplished in the light of specifying two major characteristics, including (i) risk and (ii) vulnerability sources. A risk source leads to the occurrence of a risk event when it successfully exercises a specific vulnerability within the system, or in

other words, if no vulnerability exists, no further risk events attributed to a risk source can occur. The vulnerability is highly dependent on risk probability [33,34].

To assess risks within an organization, it is critical to collect all potential risk sources. Accordingly, risk identification is highly entangled with characterizing a system to establish a clear understanding of the current situation. Hence, the associated managers should be equipped with well-organized system information. Such information includes those associated with:

- Software development, implementation, and post-implementation;
- System interfaces (e.g., internal and external connectivity);
- Data and information within a system;
- People who support and use IT systems;
- System and data criticality (e.g., the value of the system or importance to an organization);
- System and data sensitivity;
- System security policies (organizational policies, federal requirements, laws, industry practices);
- System security architecture;
- Information storage protection;
- Data availability, integrity, and confidentiality.

In addition to such areas within which the potential risk sources may pose vulnerabilities, humans with potentially harmful motivations are also able to act as a risk source, especially to be engaged in fraud. This will be discussed in further sections.

As previously mentioned, vulnerabilities associated with a system environment should be identified to provide a complete risk identification. The main objective here is the determination of potential weaknesses and vulnerabilities that a specific risk source may take advantage of and be triggered by. Such objectives can be obtained in various manners, including the ones that are mostly involved with the development of security-based controls.

The provided information associated with the risk and vulnerability sources contributes to the establishment of a strong base for further characterizing the system and also identifying the threats. However, several important factors should be considered in identifying risks associated with a project, while in most cases, being underestimated by project managers leads to failures in a project. The first and maybe the most important factor in this regard is the risk event. As mentioned in the previous section, one of the aspects of risk is the event through which an explicit and thorough description of the project will be provided. In many cases, an incomplete understanding of the risk event leads to unfulfilled risk identification through which a considerable range of risks with significant impacts may be ignored through the process. Hence, risk events are the most influential when an in-depth and clear description of events is provided through which the potential occurrence and the quality of its influence are specified. In addition to an in-depth description of the risk event, the organizational environment and the risk management plan also play key roles in conducting risk identification. These factors create and delineate the environment through which the risk evaluation will be accomplished [25,34,35].

There have been many tools and methodologies developed and utilized for risk identification, and their application may vary according to the associated project. Some of the most commonly applied tools are questionnaires, documentation reviews, diagramming techniques, information-gathering techniques (e.g., SWOT analysis), automated scanning tools, assumptions analysis, and checklists.

5.3. Qualitative Analysis

Throughout the risk identification process, well-organized documentation regarding the risks of the project are provided, which requires further analysis to organize, classify, and determine the final impact of the identified risks on the organization. Within an information system, the information related to the system's data sensitivity and criticality is crucial to accomplish associated classifications and impact determination. The analysis

of the information obtained from risk identification can be accomplished in qualitative or quantitative methods. However, throughout the identification process, the qualitative analysis precedes the quantitative one [25].

Risk qualification is fundamentally composed of several main phases. The first phase is to determine the risk baseline. As mentioned, one of the main aims of qualitative analysis is to stratify and organize the risks in projects. Baselining the risk would place any risk between absolute uncertainty (zero and 100 probability), which is the first and the best effort to stratify risk with respect to its characteristic probabilities and impacts. The process is simplified by determining total success and total failure, which allows a clear understanding of the full range of possibilities [36].

The next phase in risk qualification is rating the risk. An assigned degree to a specific risk reflects the risk analyst's character, and not all analysts have the same remarks over the degree of the risks. Accordingly, risk rating schemes are created to significantly minimize the associated discrepancies. The degree of risk is a reflection on the occurrence probability and also the impact severity. Thus, defining a risk turns out to be the matter of identifying impacts, specifying scale, and then shaping the boundaries. As the risk-rating scheme is thoroughly defined, assessing and qualifying each specified risk could be established via this structure [24,36].

Risk identification is accompanied by identifying and validating specific assumptions, which will go under further testing and analysis in the next phases of risk qualification. This testing is accomplished to validate and assess the stability and consequences. During the stability assessment, the potential of a given assumption for alteration is taken under investigation. This assessment is carried out since the nature of assumptions is not stable, and the level of their stability should be specified. In addition, the invalidation of considered assumptions should be taken into account, and the governed impacts should be clearly assessed. The associated qualification of risk is widely carried out using specific models developed for the enhanced analysis of risks. The detailed discussion of developed models is beyond the scope of this paper; however, it is noteworthy that these models support the development of risk ranking and comparative analysis [24].

As other key phases in qualitative analysis play major roles in providing accurate and functional results, the data quality evaluation, risk categorization, and urgent risk assessment should be accomplished. It is clearly recognized that the appropriate data quality improves the validity of risk qualification. These critical qualifications provide significant outcomes during the analysis, including:

1. Ensuring the validity of data sources to include them further in the process;
2. Specifying the areas of risk with varying degrees of concern/attention;
3. Determining the urgency of a given risk which delineates an appropriate vision over the time-dependency of an action.

Although most projects will include some mandatory quantitative risk analysis studies within their scope, the daily risk management inherent to each project is often overlooked in terms of formal qualitative risk analysis requirements. Managing this type of risk typically requires ongoing collaboration between project team members and the organization of regular risk review seminars. The methods used in qualitative risk analysis can vary significantly, depending on the type of project underway and the risk management resources available for the project. In this article, we consider four of the most useful qualitative risk analysis techniques applied in project management, which include the Delphi technique, SWIFT analysis, decision tree analysis, and bow-tie analysis.

The Delphi technique is a type of risk brainstorming. However, the main difference between this technique and traditional risk brainstorming is that the Delphi technique uses expert opinions to discover, analyze, and assess risks individually and anonymously. Each expert then assesses the risks of the other experts, and a risk register is created through continuous evaluation and consensus among the experts [37].

Another qualitative risk analysis is the SWIFT analysis which stands for "Structured What If Technique". SWIFT takes a systematic team-based approach in a workshop envi-

ronment where the team explores how changes to an approved plan or design might affect a project through a series of "what if" considerations. This technique is particularly useful for assessing the sustainability of opportunity risks.

Decision tree analysis is regarded as another powerful technique that is most commonly used to determine the best course of action when the outcome of possible planned events or plans is uncertain. This is achieved by starting with the original proposed decision and mapping the various pathways and outcomes as a result of the events of the original decision. Once all the routes and outcomes have been established and their respective probabilities evaluated, a course of action can be selected based on a combination of the most desirable outcomes, associated events, and odds of success [38].

Along with the abovementioned qualitative tools, bow-tie Analysis is regarded as one of the most viable techniques available to identify risk mitigation. Bow-tie analysis begins by looking at a risk event and then projects it in two directions. All possible causes of the event are listed on the left, and all possible consequences of the event are listed on the right. It is then possible to identify and apply mitigations (or barriers) for each of the causes and consequences separately, effectively reducing both the probability of the risk occurring and the subsequent effects if the risk occurs nonetheless [39].

5.4. Quantitative Analysis

Qualitative analysis provides a base for further quantification of risks attributed to the risk examination via assigning mathematical values to the project-associated risks. The main objectives of risk quantification are to increase the probability of achieving project aims, to pursue in-depth "what-if" evaluation, and to validate contingency reserves. The inputs to risk quantitative analysis include information from the risk qualification and statistical data from organization which, throughout their quantification, several tools are utilized by managers, including:

1. Interviewing technical experts to rate and rank risks in a quantitative manner;
2. Using the expected monetary value (the result of multiplying probability and impact of risk to obtain a novel quantitative parameter);
3. Decision trees through which rich information is presented in an easy-to-interpret format;
4. The program evaluation: Embedding multi-data-point duration estimates in network systems to provide specific risk values for schedules;
5. Risk Simulation tools, e.g., Monte Carlo method.

Since information development and data security are pivotal factors in information systems risk management, analyzing the impact of identified risks within an information system should strictly consider such concepts. The impacts associated with information and data security are largely reflected in the loss of data availability, integrity, and confidentiality. Accordingly, by analyzing the associated security goals, sets of helpful information can be obtained through analyzing the level of protection employed to maintain data availability, integrity, and confidentiality [34].

Data integrity is considered a critical requirement in any information system aiming to ensure no inappropriate modification is established either by intentional or accidental acts. Unwanted modification within the system or data, if not being corrected, can strongly contribute to dysfunctionality and also provides vulnerabilities for further risk resources, including fraud, inaccuracy, and risky decisions. Integrity violation can substantially pave the way for the further violation of data availability and confidentiality. It is critically important because the violation of a system or data availability can, in turn, bring about substantially mitigated operational effectiveness and functionality within an organization. Such mitigated operational effectiveness can also be reflected in the loss of confidentiality within a system through which unauthorized, unanticipated, or accidental disclosures have occurred [34,35,40].

Technically speaking, there are five fundamental risk measures, and each gives a remarkable method of evaluating the risk implied in the venture viable. The five measures

incorporate alpha, beta, R-squared, standard deviation, and Sharpe ratio. Risk measures can be utilized separately or together to conduct a risk evaluation. When looking at two likely ventures, it is shrewd to compare such to figure out which speculation has the most serious danger. Alpha and beta are the two main measures used to evaluate the performance of a portfolio of stocks, funds, or investments. Alpha measures the amount of an investment that has returned relative to a market index or another common benchmark against which it is compared. Beta measures the relative volatility of an investment. This is an indication of its relative risk. The fund should move in lockstep with the benchmark if its beta is one. Betas below one are seen to be less stable than the benchmark, whereas betas above one are thought to be more erratic.

R-Squared calculates the percentage of an investment's movement that can be attributed to changes in its benchmark index. The relationship between the investment under consideration and its related benchmark is represented by an R-squared number. The standard deviation is a way of quantifying data dispersion in relation to the dataset's mean value, and it offers a measure of an investment's volatility. The standard deviation is a measurement of how far a return-on-investment deviates from the anticipated normal or average returns. The Sharpe ratio measures performance adjusted for the associated risk. It does this by removing the rate of return on a risk-free investment, such as a US Treasury bill, from the rate of return experienced. This is then divided by the standard deviation of the related investment and serves as an indicator of whether the return on the investment was due to prudent investment or excessive risk-taking [41].

5.5. Planning Risk Response

Throughout the risk management process, developing a risk response is critically important since it specifies what response should be carried out to address particular issues identified, qualified, and quantified in previous steps. Through this step, two characteristics should be determined, which are the risk thresholds and risk causes. Determining thresholds for risk contributes to ensuring no time is wasted by excluding the intolerable approaches. In addition, specifying the risk enables managers to identify any specific reason that may reflect common risks [24,42].

It is clearly recognized that when talking about risk, it can be referred to both threats and opportunities. Accordingly, there should be associated responses to both aspects of risk. These response strategies are shown in Figure 3.

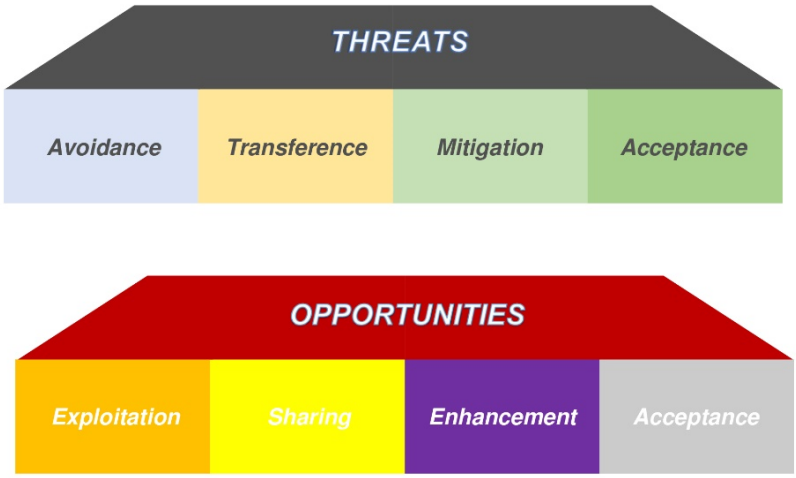

Figure 3. Aspects of risk.

One of the potentially important practices that an organization can engage in through avoiding further risk occurrence is identity management and access control. Identity management and access control is the standardized discipline in management attempting to strictly control accessibility to organizational resources to ensure the security of data and

systems. This is critically important because information and data are pivotal elements within an information system. Through these practices, the user's identities are clearly verified prior to giving them the right level of access to data and information. Identities are referred to as sets of unique attributes which differentiate a user from other users and are majorly manifested as security numbers specifically determined by the upper managers involving the titles and the associated roles of users within the organization [43].

Within this concept, there are several layers of security processes. After users register within the company, specific attributes assigned to them are collected and established within the database. These associated attributes are key factors in determining the power of a user and its flexibility within an organization. Accordingly, the control and management of the associated identities granting power to the users are critically important. After managing and specifying the identities, they are fully established through authentication. The authentication of a user can be established via different means such as an electronic identity, an electronic signature, or more simplified forms such as a full name. After the establishment of an identity, an access control decision should be pursued. In this step, the evaluation and decision over the delivered attributes are accomplished, and the access level of the user is specified. Hence, there is a subtle difference between the two layers of security, identity management and access management, where identity management is concerned with controlling and regulating the user attributes while access control is concerned with evaluating the associated attributes according to the policies and further engaging in final decisions [43,44].

The establishment of identity and access control within an organization can largely contribute to mitigating the risks associated with data development and data security. This can bring about specific challenging issues for IT admins coupled with a further frustrated user base. Accordingly, identity management and access control can be significantly effective in tracking and regulating particular accounts in having access to sensitive data coupled with securing data with correlated immune authentication practices. There have been several specific secure authentication practices employed in information systems in which single sign-on authentication is one of the simplest attempts in the field. Single sign-on is an authentication scheme enabling the user to log in once and access the organization resources without further re-providing the authentication factors just via a single identity and password. In an attempt toward providing more security, the single sign-on scheme can be further integrated with other approaches such as adaptive multi factor authentication, through which particular additional factors are required during the authentication process aiming to eliminate the risks associated with single identity authentication. Throughout this sort of authentication scheme, a real-time risk rating is also integrated into the authentication process by which conditional access is established. It also enables users to access systems and data via single authentication through which seamless access to the resources without any password is established. These practices can significantly contribute to the higher security and mitigated risks associated with conventional access routes [43,44].

Along with mitigating the risks associated with data security and access, identity management and access control can largely contribute to reducing the risks correlated with the roles changing through which the organization should regularly allow, modify, and revoke the access of users as they leave or enter the organization. This is called life cycle management, in which these role-changing tasks are automated in a highly secure and smooth manner [45,46]. Along with the schemes developed in the authentication security layer, other protection mechanisms and practices in preventing unauthorized access to system and data resources can be implemented, including mandatory access control (MAC), discretionary access control (DAC), rule-based access control, physical access control, role-based access control, attribute-based access control, and policy-based access control, which are beyond the scope of this book chapter to discuss. However, the functionality and effectiveness of each approach are highly dependent on data regulations established by the organization [43,47].

5.6. Risk Control

The last step in risk management is to implement the identified, qualified, quantified, and specified responses in action. In this regard, there are a couple of major challenges that should be taken into consideration which are (i) implementing risk plans and ensuring their validation. Risk plans should be self-fulfilling if the associated strategies and plans have been integrated. In addition, ensuring the validation of plans involves the extensive and sustainable tracking of both the risk and the environment, which is majorly accomplished through pursuing inquiries. (ii) Providing well-organized and meaningful documentation to further process support. In this step, various tools are utilized to evaluate the specific and delicate requirements of risk monitoring, including earned value analysis [24].

6. Risk Policies and Continuity Planning

Managing risks is tightly involved with policy analysis. In fact, the policy is attributed to a principle or a plan to lead decisions through obtaining intended outcomes, which are specifically applied to a broad range of subjects, including organizations, groups, governments, and individuals. Accordingly, the development and implementation of policies, aiming to guarantee continuous development, are accomplished through a similar structure as for the risk management structure, including:

1. The recognition of a problem;
2. Applying particular analysis;
3. Processing phase, including developing policy instrumentation, consulting, and coordination;
4. Decision-making;
5. Execution;
6. Final evaluation (assessing the effectiveness of the policy).

Each company or business is highly threatened by unpredicted business interruptions and associated challenges. Depending on the specific circumstances of any business, there are many particular events that might constitute a crisis. Unplanned events can bring about serious and catastrophic effects on a business, including damaging stocks, losing customers, and bankruptcy that also makes it impossible for the organizations to withstand them. These events are mainly specified by low probability, considerably large consequences, vagueness, and short response times. The crises that an organization may encounter can cover a wide range, including physical crisis, personnel crisis, information crisis, reputational crisis, criminal crisis, and economic crisis. Accordingly, it is critically important to set specific rules and policies to help to be completely immune against potential crises [48,49].

Digitalization also plays a crucial role in the continuity of an organization. The potential to treat and prevent risk, to be receptive to new ideas, and to adopt digitalization to improve efficiency and performance within the organization are all directly related to business continuity. Digital technologies allow the creation, quantification, and distribution of data required to implement new business processes to start organizing for effective implementation in a digitalized era. They can also be a very useful tool to help manage disaster risk at all stages, such as identifying and assessing, preventing, and preparing for recovery [50–52].

Business continuity planning refers to the development and maintenance of specific frameworks, policies, and established standards not only to manage a business disruption but also to create resilience [53]. It is simply understood that every business strategy is dependent on business sustainability, and each factor that violates this pre-established assumption would seriously contribute to impinging the business potential to hit its targets. Business continuity refers to the maintenance of unhindered availability and accessibility of all chief resources required for a business to act appropriately day in day out. A process of establishing a system of prevention and recovery from threatening interruptions is simply referred to as business continuity planning which its main objective is to provide the ability to preclude, prepare for, react against, and recover specific vulnerable sectors

from an unplanned event. The associated business continuity plan is an outcome of the business continuity management process, which is referred to as a management process with specified steps to reach the main objectives of a continuity plan. Businesses that participate in continuity planning exhibit much more resilience, immunity, and stability against a series of emergencies, disasters, and associated unplanned events [48,54,55].

Although used interchangeably and exhibiting common features, business continuity planning and business continuity policy are not exactly the same. In fact, along with addressing exclusive requirements for maintaining continuity, they serve different objectives within a company. The policy determines specific standards and benchmarks, while the role of a plan is to delineate how an organization reacts and behaves through an event, from its beginning to the end. It is clear that, the information required by the business continuity policy should be included in the business continuity plans [48,54,55].

A continuity plan should be concise and straightforward. There are three main steps for creating and applying a business continuity plan in an organization:

1. Risk assessment and associated analysis;
2. Development and documentation of a business continuity plan;
3. Testing and implementing a business continuity plan.

The first step in applying continuity planning in an organization is to pursue risk assessment, to determine the essential business functions, and to identify the degree and the level of the exposure to threats. Throughout this step, the critical functions required for the operation of an organization and their associated impact after their loss are identified. A robust business impact analysis focused on functionality, services, and revenues is the foundation of a successful business continuity strategy [56,57]. Critical functions of a business are mainly referred to as the business outputs that, along with lacking scheduling plasticity, impose serious implications over many organization sectors if disrupted. In fact, not all operational sectors of an organization are required to be considered as critical functions because it is highly dependent on the duration of the emergency. Accordingly, the critical operative function of each sector with respect to covering time frames should be accurately considered. Their impact on the business should be determined during the process, along with specifying the correlated critical functions. Identified critical functions should be prioritized with respect to their associated impact, aiming to establish a priority over the recovery process. During the process, after identifying organization functions, the associated processes and operations of the business should be classified with respect to their priority, including critical, important, and non-critical, as is shown in Table 1 [58]. In accordance with the process, after identifying the associated critical functions, specific people should be allocated for each one to be in charge of them [36,37].

Table 1. Classifications to prioritize business processes in continuity planning [58].

Classification	Description	Recovery Timeframe
First Priority (referred as essential)	Essential functions that are critical to be performed in practice	It commonly takes more than 48 h to recover after the disaster is declared
Second Priority (referred as significant)	Critical functions to be performed based on the schedule and after the completion of essentials	It commonly takes three to seven days to recover after the disaster is declared
Third Priority (referred as non-essential)	Less critical functions in terms of time that can improve main operations	It commonly takes eight to thirty days to recover after the disaster is declared

After specifying the critical functions of the business, a risk analysis should be accomplished over them. It is important to engage in risk assessment activities because the governed recovery plan is indeed highly dependent on the characteristics and the level of identified risk in each operation. The process of risk identification and analysis is quite

similar to what has been mentioned in the risk management structure that is also tightly involved with the qualitative and quantitative analysis.

The second step in applying continuity management is developing and documenting a continuity plan. After assessing the risk fields and their potential impact on the business under investigation, a continuity plan should be developed to determine the thresholds at which the business can accept the risks and specify the required actions against different levels of risk. At this level, there are three main actions that a business can perform according to the previous risk assessments, including:

- Accepting the existing condition;
- Diminishing the impact of a specific crisis/risk down to a satisfactory degree;
- Diminishing or eradicating the potential effects.

Among the three mentioned options, activities associated with decreasing the likelihood or impact of a disaster are more often suggested since the exposure of the business is considerably diminished to a reasonably practicable level. Accepting the present condition is mostly reflected in the fast recovery ability. However, this may not be quite effective after completing the recovery; the business may not still recover its customers or other resources used to deal with. In addition, it is found to be extensively expensive to eradicate the associated potential effects.

Accordingly, concerning the obtained information from previous assessments, strategies for continuity of the business should be developed and documented to be further validated. To develop strategies that support business continuity, several main actions should be accomplished. As an important attempt during the process, the main communication channels that are essential for emergency conditions should be determined. This includes the particular locations and personnel required to be accessible, the means to communicate, and the time characteristics of communications during an emergency. This is an essential step in developing a plan for continuity management since communication plays a critical role in all essential operative sectors of an organization [54,55].

Once the communication channels and their correlated characteristics are thoroughly identified, essential resources required for the recovery process during the emergency should be specified. This includes the determination of the following requirements:

- Minimum number of personnel required for critical operative sectors;
- Minimal requirements for implementing critical functions regarding alternate manufacturing, warehousing, operating systems, etc.;
- Means and resources of obtaining required materials;
- The time frame through which each of these specified actions are required;
- Recovery alternatives.

After identifying essential resources for the recovery process during emergencies, action over the disaster assessment should be carefully pursued. During this step, managers should identify the constituent components of disasters correlated with a particular operation, determine the means to quantitatively evaluate an emergency, and specify the main resources for obtaining information regarding the disasters under investigation. This assessment provides necessary information for decision-makers to engage in decisions. Decision-making for disasters should be included in the plan. During the process, it is important to envision the sequence of actions during and after the emergency. The decision-making process is reflected in many aspects of the business-critical functions, including the teams that are required before, during, and after the disaster, the correlated roles and responsibilities, and the time point through which these elements take action [54].

After developing strategies in continuity management, it is important to provide these strategies as documents to be applicable in further steps in crisis management. However, this documentation process should be performed since poorly written plans can be strongly frustrating, hard to be employed, and outdated in a short period. Documentation should proceed to support the quick and straightforward perception and better success in its im-

plementation. Accordingly, along with being brief and to the point, serious considerations should be taken into consideration, including:

- Well-organized writing formats to contribute to the cohesiveness and conformity of the plan;
- The specific assumption on which the strategies might be relied on should be written;
- If the planner encounters difficulty in preparing the plan, it may pertain to the fact that he/she is trying to plan for areas that do not need to be planned.

The associated documented continuity plans are further required to be tested and validated. Efficient organizational contingency management is possible if the company consistently tests the involved person's experience and knowledge of emergency response, as characterized in business continuity plans, to implement business continuity, identify and prioritize resources, thereby steadily developing the resources involved in the emergency response process and ensuring coordinated actions throughout crises, while taking technological developments and company specifics into account [59,60].

Accordingly, specific procedures should be considered to validate and test the previously documented continuity plan, including checklist tests, simulation tests, and parallel tests. Throughout the validation process, the compatibility of backup procedures is specified, the modification spots on the plan are determined, the potential of the organization to recover after a crisis is demonstrated, and a regular basis for the validation of the plan provides the opportunity to regularly update and correct inconsistencies that have been outlined. In fact, this step is highly functional as it establishes the guarantee that all important steps throughout the plan are included. As the plan is documented, adjusted, and validated, the top managers should specify a plan to implement it, which requires sets of practices such as personnel training to ensure its smooth and unhindered application within the system [48,54,55].

7. Risk Control and Fraud Detection

All businesses are threatened by fraud all over the world. During tough economic situations, small and medium-sized enterprises are more inclined toward developing ways to establish further innovation, development, and survival rather than risk management and associated activities. In addition, a highly linked world has resulted in advancements in communication and digital technology. Various forms of networks have evolved, including social media, e-commerce websites, blogs, industry trade networks, telecommunication networks, banking networks, and insurance networks, all of which generate an increasing amount of data. These networks provide a large amount of information that can be accessed anonymously, making them ideal platforms for spreading false information, mischief, and misdemeanors: fraudsters and attackers can hide their harmful actions within the mountains of data. As these networks continue to spread, fraudsters' possibilities to manipulate them for their own gain have grown as well [61,62].

Hence, along with requiring a great deal of hard work and research, they are highly endangered to fraud. Fraud commonly includes actions such as conspiracy, embezzlement, money laundering, and corruption, and it is mainly referred to as the untruthful and illegal actions committed by specific individuals or companies to provide a profitable, mostly financial outcome. Fraud occurs when an organization attempts to obtain something of value, in most cases money or property, in an illegal manner. Accordingly, fraud can originate from different sources, including staff members, suppliers, customers, and third parties having no direct connection with the associated business [25,26,63].

No single reason can be considered as the associated driving force to fraud, and many elements that may contribute to the fraud happening include motivation and the required potentials of offenders, the technical and professional ability of the fraudster, final consequences of fraud discovery, etc. However, there is a generalized model to indicate the reasons for fraud that considers the main aspects of fraud is the fraud triangle which presents three main elements as the main driving forces contributing to fraud, including motivation, opportunity, and rationalization [63,64].

Briefly, motivation which is interchangeably known as pressure, refers to the inclination of an organization towards committing fraud. In simple terms, it typically relies on either greed or need. Incentives toward committing fraud may be reflected from the personal motivations, investors, or higher-positioned managers' expectations or associated bonuses.

The opportunity is simply attributed to the conditions that enable fraud to occur. Based on numerous studies, it is indicated that employees are either completely honest or completely dishonest. However, most of the employees fall into a third category where they are mostly affected by opportunities. Among all three fraud elements, it is accounted as the only element that a company implements complete control over. The establishment of fraud opportunities mainly originate from inadequate accountant policies and weak internal controls. In other words, fraud opportunities are more likely to develop where weak internal controls, low security over properties, and imprecise policies exist [63,64].

Rationalization is the individual or organizational justification to commit fraud. The common rationalizations that fraudsters contribute to are justifications such as "the upper positioned managers doing as well" and "having no other solutions" [64].

Many studies are being carried out in an attempt to estimate the exact scales and costs that fraud poses to a business. However, most of the frauds remain unrecognized, and even if recognized, they are rarely reported. Although gaining a full understanding of the concept and compiling associated reliable statistics is involved with high complexity, it has been majorly demonstrated that fraud, along with being prevalent within an organization, can bring about serious, costly problems (explaining examples of the scale) [64]. Even if the optimistic prognosis of a long-term drop in fraud is correct, the trend is unlikely to be unstoppable or consistent. Informational and behavioral frictions, greater institutional skepticism, and economic inequality are all variables that might hinder the long-term drop in fraud [65–67].

Aside from the vast scale of problems and costs that fraud can impose on a business, a great number of organizations all over the world still lack formal systems and processes aiming to detect, prevent and respond to fraud. In this regard, managers who professionally deal with the analysis of information and systems can play a chief role in the establishment and accomplishment of such systematized anti-fraud activities within an organization. There has been a great attempt toward employing integrated (or hybrid) multiple-criteria decision-making methods by modern decision-makers in acting against fraud and fraudsters [68,69]. Accordingly, financial organizations are increasingly relying on data-driven strategies to build fraud detection systems that can detect and prevent illegal transactions automatically [70–72]. Generally, along with the development of anti-fraud actions, specific approaches should be developed to prevent fraud, detect, and respond appropriately [64].

Considering the prevalence of fraud in numerous organizations and its associated destructive consequences, there is a compelling argument concerning the engagement of organizations in anti-fraud activities, which requires investing time and other resources. Generally, the anti-fraud strategies can be classified into four main actions as the following:

1. Prevention;
2. Detection;
3. Deterrence;
4. Response.

Each of these anti-fraud strategies are highly interconnected, and each one contributes to a particular role in eliminating fraud from an organization [73].

7.1. Fraud Prevention

According to elements that contribute to fraud, it is clearly recognized that some effective ways should be performed to prevent fraud. These ways are mainly correlated with decreasing the associated incentives, mitigating the required opportunities, and restricting the ability of potential fraudsters to rationalize their fraud actions. Associated prevention methods mainly include the establishment of policies, controls, and practices,

including training and fraud awareness to halt fraud from occurring. Here, we are discussing several main preventative efforts to mitigate the occurrence and cost of fraud within an organization [63,64].

One of the most critical factors contributing to anti-fraud activities is to create a well-organized ethical organization within a business [74]. More dynamic and proactive managerial efforts, such as building an "ethical tone at the top" and establishing an efficient "ethics training", are necessary to construct a whistleblowing policy in a firm, which in turn positively influences employees' impressions of corporate anti-fraud tactics [74,75]. The attitudes within an organization can largely determine the extent to which the organization is likely to be at risk of fraud. Ethical standards have been revealed to be very beneficial in the long run and in very different aspects since many people, including customers, suppliers, the community, etc., realize that they can rely on a trustworthy organization with well-established ethical standards. The definition of well-organized ethical standards is not quite clear, and it can vary from organization to organization. However, in standardizing an ethical policy, it mostly attempted to establish straightforward short enough statements for better efficiency [63].

In some references, it is recommended to develop and promote ethical codes, which refer to particular policies concerning ethical conduct and implementation within an organization. However, such documented ethics codes are not sufficient to effectively prevent this. In fact, these ethical standards should be tightly entangled within the organizational culture. Accordingly, the commitment to ethical behaviors should be primarily reflected in the behavior of upper-positioned managers because within an organization the employees are more likely to imitate what they see from their superior managers. In addition, alongside the commitment of the senior managers, they must contribute to controlling the fraud risk and establish activities that may help to grow an anti-fraud culture [63,64].

Another important activity that an organization should perform to manage and prevent fraud risks is the regular assessment of fraud risks. This assessment is carried out in a similar manner discussed previously in the risk management section. Simply, the fraud risks should be clearly identified in all aspects, directly-related and indirectly related, and further assessed concerning their impact and probability.

Identifying and assessing fraud risks provide a wealth of information for further establishing the training to increase the awareness of individuals within an organization. The necessity to increase the awareness of an organization in terms of fraud is more obviously recognized since, after the occurrence of fraud, those who have been close to the fraud surprisingly declare a low consciousness concerning the fraud. Thus, as an imperative step through the risk management process, it is essential to increase the awareness of individuals within an organization through formal training, group meetings, posters, newsletters, bulletins, and associated platforms. Through this training, employees would be enlightened on what constitutes fraud, how to prevent and identify fraudulent behavior, how to respond if it has happened, and hence, the communication should be constantly established [64,76].

Just as employee awareness raises, it should be widely established in an organization as a major component of fraud risk management and an effective reporting mechanism. The importance of establishing an effective reporting system is simply understood since most of the employees are aware of specific misconducts in the organization, and a large set of them may remain silent. This silence in reporting such misconduct is majorly reflected in many conflicting emotions, including working group/family loyalties, fear of consequences, and suspicion rather than proof. Accordingly, the senior managers should provide a culture through which all employees play an important role in fraud-fighting [76].

Another significant approach in developing a preventative culture within an organization is to provide a well-organized internal control system.

7.2. Detecting Fraud

It is of significant importance to invest time and resources to develop and establish approaches required for fraud prevention within an organization since it strongly supports the further sustainability and continuity of the business. In addition, the recovery of an organization after the occurrence of fraud is a highly inefficient and time-consuming process, and most organizations cannot fully recover the losses they have had. Nevertheless, the methodologies developed for preventing fraud are unable to ensure complete immunity to an organization. Accordingly, an organization should engage in other specific policies to ensure that the continuity of the system would be established after the fraud happened. This is mainly met through fraud detection. Fraud detection methodologies usually employ specific procedures that mostly rely on analytical approaches and reporting systems to specify and sum up the existence of inconsistencies and anomalies [63,64,76].

Generally, fraud can be detected and revealed in several main ways. Since the risk management process plays a substantial role in fraud management, the internal audit functions should be strictly established to monitor risk management activities and fraud-susceptible factors. Moreover, the associated controls and mechanisms established within an organization largely contribute to fraud discovery. Aside from the fraud-related considerations, fraud can also be detected by accident or in terms of received information. However, concerning the fraud discovery, two sets of elements are considered to be highly helpful, including (i) warnings and fraud indicators and (ii) tools and methodologies [63].

As mentioned, no systems are fully fraud-proof, and there is always a possibility of fraud occurrence. Accordingly, identifying fraud indicators can provide great potential in early diagnosis and discovery. There are two main classes of fraud indicators include alerts and warning signs.

Warning signs are known as the organizational indicators of fraud risk, which can be reflected in different areas of business risk, financial risk, environmental risk, information systems, and technology risks.

7.3. Fraud Deterrence

Although stated separately as a different anti-fraud strategy, deterrence is highly interrelated with the prevention concept. Fraud deterrent is a proactive, preventative strategy, whereas fraud detection is a reactive reaction to either a misuse of assets or falsification of financial results. Effective preventative measures act as powerful deterrents to individuals who would otherwise be inclined to perpetrate fraud [77,78].

Fraud detection serves as a deterrent to potential fraudsters by notifying them that the firm is actively counteracting fraud and that systems are in place to identify any illegal conduct that has happened. The fear of being caught will often prevent a potential criminal from attempting fraud. Additional detection controls should also be put in place to compensate for the fact that deterrent measures may be ineffective in some cases [64,77].

Three basic elements are essential in the prevention of fraud. To some extent, they all entail elements of a solid ethical culture: top management's action-based commitment to ethical behavior, heightened skepticism and an inquiring attitude, and powerful communication from all those associated with the financial reporting process [79].

A. Senior management's solid commitment to ethical behavior must be supported by acts as well as words. It has often been demonstrated that simply establishing a written code of ethics is insufficient to avoid ethical misconduct. Such enormous codes are widely acknowledged to be merely a showpiece that does not influence behavior [80].
B. Skepticism is widely recognized in audit procedures as a fraud deterrent; however, it also plays an essential role in financial reporting. Skepticism manifests itself in people at all levels of the accounting profession and encompassing specific characteristics including:
    - Accounting professionals consider all elements of economic activity rather than just accepting the first certain response or what someone in authority

states. That is why they have a questioning mind that leads to suspending final judgment and seeking more information and backup.
- Interpersonal knowledge assists accountants in recognizing that people's views and reasons for reaching a specific result might be skewed.
- Accountants with integrity and determination to make their own decisions, along with self-confidence, can determine and research matters for themselves rather than accepting the assertions of others.

C. Finally, effective communication among participants in the financial reporting process is critical for fraud prevention and deterrence. It is the inevitable outcome of a strong ethical culture; however, it is still worth mentioning. Understanding any extra data that supports accounting findings can assist in preventing or eliminating the suspicion of misconduct when no illegal or unethical activity exists. In other words, improved communication enables everyone involved in the process to have a better understanding of the logic and evidence that underpin accounting choices and conclusions. As a result, there is less guessing and speculation while making an effort to comprehend intentions [79].

7.4. Responding to Fraud

A formal approach to address and handle detected or suspected cases of fraud is to employ a plan called the fraud response plan. By using this plan, corporations can gather evidence to facilitate the response to fraud in a legal manner. Moreover, the corporate fraud response plan lowers the tendency to commit fraud which not only results in minimum loss and damage but also builds up market confidence and integrity of evidence for organizations [63,64,80].

Generally, the fraud response plan is what creates legal, ethical, and moral standards for activities, and in the case of standard violation, the plan helps the organization to take any action against that person. All members of staff, and other stakeholders (customers, suppliers, and shareholders), must be aware of the fraud response plan, which contains the standards and the consequences of not respecting them. Although publicly exposing fraud has an adverse effect on the company's public image, it is a warning to those tempted to misconduct. Thus, regulated financial services companies are now legally obliged to report financial crime [64,76].

Roles and responsibilities in an organization are contingent on the size, industry, culture, and other factors. Generally, managers and supervisors are responsible for detecting fraud and other irregularities in their area. The finance director is responsible for the organization's response to fraud. Human resources usually handle any internal disciplinary procedures. Legal advisers (internal or external) are called as soon as a fraud is reported to advise on civil, internal, criminal responses, and the recovery of assets. If computers were used for fraud, IS and IT staff can provide technical advice on IT security, capability, and access. Public relations are in charge of preparing a brief for the press if that news of fraud becomes public. The police also investigate the matter. External consultants investigate skills from outside the organization. Insurers protect organizations against large fraud losses. Furthermore, where applicable, large organizations may have fraud officers, audit committees, and internal and external auditors [63,64,80].

Several steps are generally being employed to respond to an identified fraud. First, after recording and evaluating all required details, the fraud officer should establish an investigation team accompanied by the advisers' team. Throughout the associated investigation, objectives, time frame, and the required resources should be clearly specified. Accordingly, a formulated plan should be developed, and for each specific action, authorities should be assigned. The actions within the developed plan are majorly involved with the recovery of the stolen resources, funds, and properties coupled with the modification and adjustment of existing anti-fraud strategies to prevent further occurrence of similar fraud events [64,80].

8. Conclusions

With growing complexity in different businesses, information and data processing plays an important role in the effective operation of departments within an organization. Data processing is a substantially time-consuming effort since great and growing volumes of data exist in any organization. Accordingly, information systems in light of advances in computer-based systems have been developed to streamline the specific practices associated with data processing, specifically to collect, store, process, and analyze data, and also extract and disseminate information for particular purposes. Such information systems are largely contributing to the significant increase in the effectiveness of organizations through various means, especially in decision-making processes. However, aside from the wide range of advantages that information systems present to an organization, it has also brought a series of potential risks within an organization. Risks associated with the implementation and the development of information systems are highly involved in information development and data security. Hence, there is growing attention and investment in resources throughout the world aiming to standardize and develop specific frameworks through which the associated risks can be mitigated. These are recognized as risk management practices. Risk management provides a broad range of applications and disciplines which attempt to develop particular plans and frameworks to detect, prevent, mitigate, and respond to risks in highly organized structures. Throughout such structures, the risks are identified, organized, analyzed both qualitatively and quantitatively, and further responded to, which is coupled with developing particular policies to prevent the occurrence of similar risk events. Although there have been numerous literature studies in different fields of healthcare organizations, insurance, energy power, waste management, mining, etc., great efforts are still required to fill the gaps existing in the literature, specifically in the fields of psychological factors and social system issues causing information system risks.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Nikoloski, K. The role of information technology in the business sector. *Int. J. Sci. Res. (IJSR)* **2014**, *3*, 303–309.
2. Rochmah, T.N.; Fakhruzzaman, M.N.; Yustiawan, T. Hospital staff acceptance toward management information systems in Indonesia. *Health Policy Technol.* **2020**, *9*, 268–270. [CrossRef]
3. Mutwiri, W. *Amazon Business Information Systems. Data Acquisition and Management in Its Value Chain*; GRIN Verlag: Munich/Ravensburg, Germany, 2020.
4. Lucas, H.C., Jr. Performance and the use of an information system. *Manag. Sci.* **1975**, *21*, 908–919. [CrossRef]
5. Abe, S.; Ozawa, M.; Kawata, Y. *Science of Societal Safety: Living at Times of Risks and Disasters*; Springer Nature: Berlin/Heidelberg, Germany, 2019.
6. Juntunen, M.; Lehenkari, M. A narrative literature review process for an academic business research thesis. *Stud. High. Educ.* **2021**, *46*, 330–342. [CrossRef]
7. Zhu, T.; Haugen, S.; Liu, Y. Risk information in decision-making: Definitions, requirements and various functions. *J. Loss Prev. Process Ind.* **2021**, *72*, 104572. [CrossRef]
8. Aven, T.; Zio, E. Foundational issues in risk assessment and risk management. *Risk Anal.* **2014**, *34*, 1164–1172. [CrossRef] [PubMed]
9. Aven, T. Risk assessment and risk management: Review of recent advances on their foundation. *Eur. J. Oper. Res.* **2016**, *253*, 1–13. [CrossRef]
10. Hansson, S.O.; Aven, T. Is risk analysis scientific? *Risk Anal.* **2014**, *34*, 1173–1183. [CrossRef] [PubMed]
11. Aven, T.; Heide, B. Reliability and validity of risk analysis. *Reliab. Eng. Syst. Saf.* **2009**, *94*, 1862–1868. [CrossRef]
12. Veres, O.; Ilchuk, P.; Kots, O.; Rishnyak, I.; Rishniak, H. Development of an Information System to Minimize the Risks of Personnel Management. In *Conference on Computer Science and Information Technologies*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 939–958.
13. Chinazirova, S.; Tlekhurai-Berzegova, L.; Buller, E.; Kadakoeva, G. Development of an information system for the assessment of industrial and environmental risks of the enterprise. *Econ. Sci.* **2020**, *3*, 45–49.
14. Thompson, K.M.; Deisler, P.F., Jr.; Schwing, R.C. Interdisciplinary vision: The first 25 years of the Society for Risk Analysis (SRA), 1980–2005. *Risk Anal. Int. J.* **2005**, *25*, 1333–1386. [CrossRef]

15. Lowrance, W.W.; Klerer, J. Of Acceptable risk: Science and the Determination of Safety. *J. Electrochem. Soc.* **1976**, *123*. [CrossRef]
16. Kaplan, S.; Garrick, B.J. On the quantitative definition of risk. *Risk Anal.* **1981**, *1*, 11–27. [CrossRef]
17. AMSC; SAFT. *Department of Defense Standard Practice forSystem Safety*; United States Department of Defense, The Pentagon: Arlington County, VA, USA, 2012.
18. Aven, T.; Renn, O. On risk defined as an event where the outcome is uncertain. *J. Risk Res.* **2009**, *12*, 1–11. [CrossRef]
19. Lemos, F. On the definition of risk. *J. Risk Manag. Financ. Inst.* **2020**, *13*, 266–278.
20. Ward, S.; Chapman, C. Stakeholders and uncertainty management in projects. *Constr. Manag. Econ.* **2008**, *26*, 563–577. [CrossRef]
21. Pritchard, C.L. *Risk Management: Concepts and Guidance*; Auerbach Publications: Boca Raton, FL, USA, 2014.
22. Chen, J. Risk communication in cyberspace: A brief review of the information-processing and mental models approaches. *Curr. Opin. Psychol.* **2020**, *36*, 135–140. [CrossRef] [PubMed]
23. Humayun, M.; Niazi, M.; Jhanjhi, N.; Alshayeb, M.; Mahmood, S. Cyber security threats and vulnerabilities: A systematic mapping study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
24. Finne, T. Information systems risk management: Key concepts and business processes. *Comput. Secur.* **2000**, *19*, 234–242. [CrossRef]
25. Sherer, S.A.; Alter, S. Information systems risks and risk factors: Are they mostly about information systems? *Commun. Assoc. Inf. Syst.* **2004**, *14*, 2. [CrossRef]
26. Goldstein, J.; Benaroch, M.; Chernobal, A. IS-Related Operational Risk: An Exploratory Analysis. In Proceedings of the AMCIS, Toronto, ON, Canada, 14–17 August 2008.
27. Bank for International Settlements. Basel committee on banking supervision (BCBS). In *International Convergence of Capital Measurement and Capital Standards: A Revisedframework*; BCBS: Basel, Switzerland, 2006.
28. Tefera, A.; Bekele, B. Periodontal disease status and associated risk factors in patients attending a tertiary hospital in northwest Ethiopia. *Clin. Cosmet. Investig. Dent.* **2020**, *12*, 485. [CrossRef]
29. Westerman, R.; Kuhnt, A.-K. Metabolic Risk Factors and Fertility Disorders: A Narrative Review of the Female Perspective. *Reprod. Biomed. Soc. Online* **2022**, *14*, 66–74. [CrossRef]
30. Samimi, A.; Samimi, M. Investigation of Risk Management in Food Industry. *Int. J. Adv. Stud. Humanit. Soc. Sci.* **2020**, *9*, 195–204.
31. Stackpole, C.S. *A User's Manual to the PMBOK Guide*; John Wiley & Sons: Hoboken, NJ, USA, 2013.
32. Suroso, J.S.; Fakhrozi, M.A. Assessment of information system risk management with octave allegro at education institution. *Procedia Comput. Sci.* **2018**, *135*, 202–213. [CrossRef]
33. Stoneburner, G.; Goguen, A.; Feringa, A. Risk management guide for information technology systems. *Nist Spec. Publ.* **2002**, *800*, 800–830.
34. Boiko, A.; Shendryk, V.; Boiko, O. Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia Comput. Sci.* **2019**, *149*, 65–70. [CrossRef]
35. Longerstaey, J.; Spencer, M. *Riskmetricstm—Technical Document*; Morgan Guaranty Trust Company of New York: New York, NY, USA, 1996; Volume 51, p. 54.
36. Benjamin, C.W.; Chou, H.-Y.; Wu, M.B.; Chang, D.H. The Risks of Risk Management. In Proceedings of the 2006 IEEE International Conference on Management of Innovation and Technology, Singapore, 21–23 June 2006; pp. 708–712.
37. Chalmers, J.; Armour, M. *The Delphi Technique*; Springer: Singapore, 2019. [CrossRef]
38. Kaveh, A.; Rahami, H.; Shojaei, I. Swift analysis of linear and non-linear structures and applications using reanalysis. In *Swift Analysis of Civil Engineering Structures Using Graph Theory Methods*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 201–245.
39. Zhang, Y.; Guan, X. Selecting project risk preventive and protective strategies based on bow-tie analysis. *J. Manag. Eng.* **2018**, *34*, 04018009. [CrossRef]
40. Brown, D.F.; Dunn, W.E. Application of a quantitative risk assessment method to emergency response planning. *Comput. Oper. Res.* **2007**, *34*, 1243–1265. [CrossRef]
41. Kumar, L.; Jindal, A.; Velaga, N.R. Financial risk assessment and modelling of PPP based Indian highway infrastructure projects. *Transp. Policy* **2018**, *62*, 2–11. [CrossRef]
42. Fang, C.; Marle, F.; Xie, M.; Zio, E. An integrated framework for risk response planning under resource constraints in large engineering projects. *IEEE Trans. Eng. Manag.* **2013**, *60*, 627–639. [CrossRef]
43. Okta. What Is Identity Management and Access Control? Available online: https://www.okta.com/identity-101/what-is-identity-management-and-access-control/ (accessed on 10 November 2021).
44. Bugge, C.; Williams, B.; Hagen, S.; Logan, J.; Glazener, C.; Pringle, S.; Sinclair, L. A process for Decision-making after Pilot and feasibility Trials (ADePT): Development following a feasibility study of a complex intervention for pelvic organ prolapse. *Trials* **2013**, *14*, 1–13. [CrossRef]
45. Alsmadi, I.; Burdwell, R.; Aleroud, A.; Wahbeh, A.; Al-Qudah, M.; Al-Omari, A. Security and access controls: Lesson plans. In *Practical Information Security*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 53–71.
46. Beres, Y.; Baldwin, A.; Mont, M.C.; Shiu, S. On identity assurance in the presence of federated identity management systems. In Proceedings of the 2007 ACM workshop on Digital Identity Management, Fairfax, VA, USA, 2 November 2007; pp. 27–35.
47. Yeluri, R.; Castro-Leon, E. Identity management and control for clouds. In *Building the Infrastructure for Cloud Security*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 141–159.

48. Blyth, M. *Business Continuity Management: Building an Effective Incident Management Plan*; John Wiley & Sons: Hoboken, NJ, USA, 2009.
49. Jose, D.; Rosa, P.D.S.; Rosa, S. *Crisis Management*; Ateneo Graduate School of Business: Makati City, Philippines, 2020.
50. Moşteanu, D.; Roxana, N. Management of disaster and business continuity in a digital world. *Int. J. Manag.* **2020**, *11*, 169–177.
51. Moşteanu, N.R.; Faccia, A.; Cavaliere, L.P.L. Disaster Management, Digitalization and Financial Resources: Key factors to keep the organization ongoing. In Proceedings of the 2020 4th International Conference on Cloud and Big Data Computing, Liverpool, UK, 26–28 August 2020; pp. 118–122.
52. Moşteanu, N.R. Challenges for Organizational Structure and design as a result of digitalization and cybersecurity. *Bus. Manag. Rev.* **2020**, *11*, 278–286. [CrossRef]
53. Fezzey, T.; Batchelor, J.H.; Burch, G.F.; Reid, R. *Cybersecurity Continuity Risks: Lessons Learned from the COVID-19 Pandemic*; Kennesaw State University: Kennesaw, GA, USA, 2021.
54. Lindström, J.; Samuelsson, S.; Hägerfors, A. Business continuity planning methodology. *Disaster Prev. Manag. Int. J.* **2010**, *19*, 243–255. [CrossRef]
55. Syed, A.; Syed, A. *Business Continuity Planning Methodology*; Sentryx: Austerlitz, The Netherlands, 2004.
56. Yang, C.-H.; Lee, K.-C. Developing a strategy map for forensic accounting with fraud risk management: An integrated balanced scorecard-based decision model. *Eval. Program Plan.* **2020**, *80*, 101780. [CrossRef]
57. Lahuta, P.; Kardoš, P.; Hudáková, M. Integrated Risk Management System in Transport. *Transp. Res. Procedia* **2021**, *55*, 1530–1537. [CrossRef]
58. Jafar, E.; Taneja, U. Business continuity planning—A survey of hospitals in Delhi. *J. Public Health* **2017**, *25*, 699–709. [CrossRef]
59. Civča, D.; Atstāja, D.; Koval, V. Business continuity plan testing methods in an international company. *Restruct. Manag. Increase Compet. Trading Co. Latv.* **2021**, *5*, 341.
60. Sasaki, H.; Maruya, H.; Abe, Y.; Fujita, M.; Furukawa, H.; Fuda, M.; Kamei, T.; Yaegashi, N.; Tominaga, T.; Egawa, S. Scoping review of hospital business continuity plans to validate the improvement after the 2011 Great East Japan Earthquake and Tsunami. *Tohoku J. Exp. Med.* **2020**, *251*, 147–159. [CrossRef] [PubMed]
61. Niemimaa, M.; Järveläinen, J.; Heikkilä, M.; Heikkilä, J. Business continuity of business models: Evaluating the resilience of business models for contingencies. *Int. J. Inf. Manag.* **2019**, *49*, 208–216. [CrossRef]
62. Setiawan, A.; Wibowo, A.; Susilo, A.H. Risk analysis on the development of a business continuity plan. In Proceedings of the 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta Bali, Indonesia, 8–10 August 2017; pp. 1–4.
63. Pourhabibi, T.; Ong, K.-L.; Kam, B.H.; Boo, Y.L. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decis. Support Syst.* **2020**, *133*, 113303. [CrossRef]
64. Hooi, B.; Shin, K.; Song, H.A.; Beutel, A.; Shah, N.; Faloutsos, C. Graph-based fraud detection in the face of camouflage. *ACM Trans. Knowl. Discov. Data (TKDD)* **2017**, *11*, 1–26. [CrossRef]
65. Karpoff, J.M. The future of financial fraud. *J. Corp. Financ.* **2021**, *66*, 101694. [CrossRef]
66. Files, R.; Martin, G.S.; Rasmussen, S.J. Regulator-cited cooperation credit and firm value: Evidence from enforcement actions. *Account. Rev.* **2019**, *94*, 275–302. [CrossRef]
67. Morgan, R.E. *Financial Fraud in the United States, 2017*; US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, NCJ: Washington, USA, 2021; Volume 255817.
68. Samociuk, M.; Iyer, N.; Doody, H. *A Short Guide to Fraud Risk: Fraud Resistance and Detection*; Routledge: London, UK, 2017.
69. Baldree, J. *Fraud Risk Management: A Guide to Good Practice*; CIMA Publisher Wokingham: Wokingham, UK, 2008.
70. Baesens, B.; Höppner, S.; Verdonck, T. Data engineering for fraud detection. *Decis. Support Syst.* **2021**, 113492. [CrossRef]
71. Stojanović, B.; Božić, J.; Hofer-Schmitz, K.; Nahrgang, K.; Weber, A.; Badii, A.; Sundaram, M.; Jordan, E.; Runevic, J. Follow the trail: Machine learning for fraud detection in Fintech applications. *Sensors* **2021**, *21*, 1594. [CrossRef] [PubMed]
72. Temuçin, T.S.; Erbaş, S.; Anıl, A. Using Big Data in Internal Fraud Detection. *TIDE Acad. Res.* **2021**, *3*, 55–82.
73. Todorović, Z.; Tomaš, D.; Todorović, B. Anti-Fraud Strategy. *Economics* **2020**, *8*, 69–78. [CrossRef]
74. Suh, J.B.; Shim, H.S. The effect of ethical corporate culture on anti-fraud strategies in South Korean financial companies: Mediation of whistleblowing and a sectoral comparison approach in depository institutions. *Int. J. Law Crime Justice* **2020**, *60*, 100361. [CrossRef]
75. Dolan, S.; Hawkins, S.; Albrecht, C.; Richley, B. Raising the ethical bar: Ethical audits and positive culture transformation. *The European Business Review*. 11 January 2021. Available online: https://www.europeanbusinessreview.com/raising-the-ethical-bar-ethical-audits-and-positive-culture-transformation/ (accessed on 10 November 2021).
76. Jackson, P.M. Debate: Fraud risk management in the public sector. *Public Money Manag.* **2013**, *33*, 6–8. [CrossRef]
77. Eusebio, N. *Anti-Fraud Strategy*; Technical Note ACCID; Associació Catalana de Comptabilitat i Direcció: Vic, Spain, 2017.
78. Sofia, I.P. The impact of internal control and good corporate governance on fraud prevention. In Proceedings of the International Seminar on Accounting Society, Kota Tangerang Selatan, Indonisea, 21 November 2020.
79. Reporting, D.F. Three pillars of fraud deterrence and detection. *Strateg. Financ.* **2015**, *96*, 17–18.
80. Araj, F.G. *Responding to Fraud Risk*; The Institute of Internal Auditors Research Foundation (IIARF): Lake Mary, FL, USA, 2015.