Digitalisation and IT Risk Management: Towards a System for Improved Business Sustainability

Bilgin Metin , Sefa Duran , Eda Telli , Meltem Mutlutürk , Martin Wynn *

Posted Date: 19 October 2023

doi: 10.20944/preprints202310.1227.v1

Keywords: risk assessment; information security; risk management; segregation of duties; security culture model; SCM; COBIT 2019; unified modelling language; ISO 27001

Article

Digitalisation and IT Risk Management: Towards a System for Improved Business Sustainability

Bilgin Metin [1], Sefa Duran [1], Eda Telli [1], Meltem Mutlutürk [1] and Martin Wynn [2,*]

[1] Department of Management Information Systems, Bogazici University, Hisar Campus, Bebek, Istanbul, Turkey; bilgin.metin@boun.edu.tr; m.sefaduran@gmail.com; eda.yamamoto@tages.biz; meltem.mutluturk@boun.edu.tr

[2] The School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham, UK

* Correspondence: mwynn@glos.ac.uk

Abstract: To proactively manage information security, enterprises often employ information security risk assessment techniques. Asset value - which is used to calculate the financial impact of possible threats - is one of the key parameters of information security risk. However, assets in a system are rarely independent, and their values are typically interdependent. Asset owners and IT teams may hold different views as regards these values, and there is thus the need to reduce subjectivity in a qualitative risk assessment. The research entails the development of a conceptual framework derived from the literature to minimize subjectivity, and the design of a system based on those concepts. The study uses the Unified Modeling Language as a design tool and puts forward an object-oriented model for defining asset values, in which the relationships between assets, vulnerabilities and related threats are identified. A "segregation of duties" approach is integrated into the risk management system to mitigate against subjectivity and better determine asset values. Survey responses from 16 practitioners working in the private and public sectors confirm the validity of the approach, but suggest it may be more workable in larger organisations where resources allow dedicated risk professionals to operate.

Keywords: risk assessment; information security; risk management; segregation of duties; security culture model; SCM; COBIT 2019; unified modelling language; ISO 27001

1. Introduction

The significance of managing IT related risk in the digital era has come to the fore in recent years in the context of cybersecurity and sustainability, and the rapid growth of the associated risks to organisations and society at large [1]. The management of IT related risk has been a fundamental discipline in most industry sectors for several decades and, within the IT function, this is often part of a Disaster Recovery Plan, which may also be viewed as an element of a Business Continuity Plan at corporate level. However, although risk management has become a significant element in some of the most widely deployed industry standard methodologies, there is no universally agreed method for managing risk. It is nevertheless clear that the application of integrated risk management methods can support early risk identification and assessment, thereby minimizing threat related costs and improving security outcomes [2]. In the USA, for example, new regulatory and compliance objectives issued by the Cybersecurity and Infrastructure Security Agency in 2022 [3] put renewed emphasis on the importance of effective asset inventory and vulnerability management. Indeed, vulnerability management is increasingly seen as an essential strategic necessity, and was recently defined by cybersecurity company Rapid7 [4] as "the process of identifying, evaluating, treating, and reporting security vulnerabilities in business processes, web applications, and systems (as well as the software that runs on them)". The company also notes that "this process needs to be performed continuously in order to keep up with new systems being added to networks, changes made to systems and applications, and newly discovered vulnerabilities over time" (p.3).

Practically all company activities come with a particular risk associated with them. Whilst not all risks are IT related, the majority of corporate risks have an IT component, usually linked to the current IT asset portfolio or the business processes underpinned by this technology. Senior

 doi:10.20944/preprints202310.1227.v1

management have become increasingly aware of the importance of IT risk management and the need to understand the risks that IT creates for a company. However, many companies prioritize the higher-profile risks to the detriment of assessing other threats and risks relevant to their business. There are a number of tools and approaches available to support risk management planning and execution, including the use of maturity models [5]. These may help companies in putting appropriate security policies in place, to reduce risks and their impacts, and to ensure all processes operate smoothly.

Risk assessment is integrally linked with business sustainability in the digital era. Many companies are using risk management methods that are not equipped to handle the complexity of IT risks associated with digitalisation, constituting a threat to business continuity, or even company survival. The scope of cyber threats is growing, and the deployment of digital technologies is a one of the main contributory causes. Carelton and Krishnamoorthi [6] (p.3) observed that organisations now have more "digital touch points" with customers and business partners than ever before. The authors cite websites, email, blogs, e-commerce sites, social media, news pages, search engines and mobile apps as potential touch points, providing an indication of the scale and scope of the issues that cybersecurity policies and measures have to recognise, embrace and resolve. They found that "cyber-criminals exploit these touchpoints to trick people into sharing login credentials and personally identifiable information (PII)", and concluded that "organizations are also struggling to stay ahead of cyber-criminals who use APIs, fuzzing, link manipulation, phishing through search engines, and other techniques to make fake websites appear authentic". This requires innovative and effective solutions if enterprises are to be adequately protected against cybercrime and IT related risks.

A risk management committee can play a key role as the "gate-keeper" to ensure appropriate risk assessment and prioritization, and effective decision-making [7], which can help address the concern of subjectivity in the assessment of risk. In this research, a "segregation of duties" approach is used for asset valuation, which is based on the principle that no individual person, role, or group, should be able to execute all aspects of the risk assessment process. Awati [8] (para.1). defines this as "an internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any task", and that this "involves breaking down tasks that might reasonably be completed by a single individual into multiple tasks so that no one person is solely in control".

This research develops a conceptual framework from which an IT risk assessment system based on a segregation of duties approach is designed, aimed at improved risk management and thus business sustainability. The Unified Modeling Language (UML) is used in the design for process representation. The paper comprises six sections. Following this introduction, relevant literature is examined in section 2 and two research questions are set out. Section 3 then outlines the research method and establishes the conceptual and framework for the system. Section 4 outlines the system design and operation, and validation and related issues are discussed in section 5. The concluding section summarises the findings from the study, and discusses limitations of the study and possible future areas of research.

2. Relevant Literature and Standards

Both quantitative and qualitative techniques can be used to assess risk, but many companies lack access to the accurate financial data that is required to use quantitative methods to assess IT asset values. For example, measures such as single loss expectancy, annualized rate of occurrence, and annualized loss expectancy may not be readily available [9]. Many organizations therefore often pursue a qualitative risk evaluation, by assigning values to IT assets, including corporate information, which is one of the most important assets of an organization [10]. This has been highlighted by the data breaches and attacks suffered by many organizations in recent years [11], and information security management is increasingly viewed as an important tool in ensuring organisational sustainability [12,13].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 October 2023 doi:10.20944/preprints202310.1227.v1

Risk analysis is an essential component of an information security management system (ISMS), which involves identifying assets, threats, and vulnerabilities as well as an assessment of the likelihood of those threats and vulnerabilities occurring. Such risks can be conceptualised as anything that may compromise the confidentiality, integrity, and/or availability of information. Risk management is the process of identifying the factors that lead to such risks and how to mitigate them. However, qualitative risk assessment involves subjective prioritization that may lead to inappropriate asset valuations that underpin important decisions regarding information security management.

The international standard ISO 27001 [14] sets out a framework for establishing, implementing, monitoring, maintaining and improving an ISMS. One of the basic principles of ISO 27001 is that the information security measures that are adopted by companies should respond to relevant threats identified by risk assessment. ISO 27001 is aligned with another international standard ISO 31000, which provides guidelines on how to organize risk management in organizations. It is not focused solely on information security risks, but rather can be applied to a wider range of business risk scenarios. Kosutic [15] has examined the relationship between the two standards and suggested the overlap of some of the main areas of risk in organisations (Figure 1). Here, we are concerned with information security risk, which encompasses all of cybersecurity and a part of information technology.

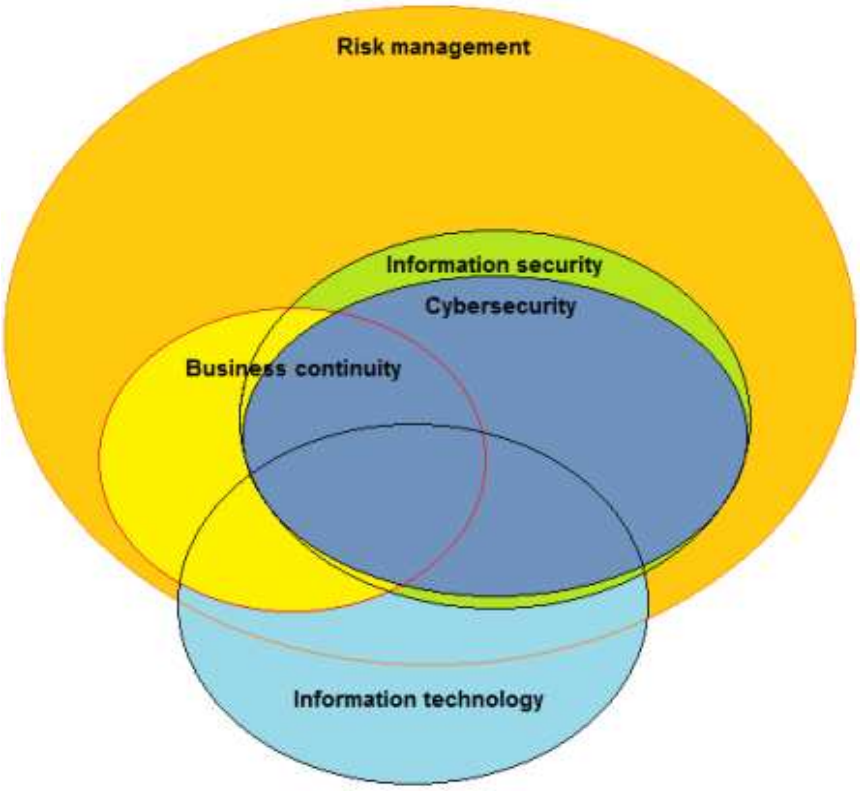

Figure 1. Information security risk and related risk areas. Source: Kosutic [15].

Risk assessment can be conducted in two ways: asset-based or scenario-based. Asset-based assessment focuses on the relevant assets (the information, systems, hardware and associated infrastructure etc.), using threat and vulnerability measures to calculate the risk [16]. Vulnerabilities are the weaknesses of the company systems, hardware and infrastructure that may allow attackers to exploit these vulnerabilities and access and harm the company systems. A threat is the potential of an attacker to be able to exploit a vulnerability. Scenario-based assessment, on the other hand, deals more with the circumstances of the threat [17]. In this context, Nost et al. [18] (para. 6) note that "modern vulnerability prioritization practices require an asset-centric approach, which is vital to identifying and remediating an organization's biggest vulnerability risks. Unfortunately,

 doi:10.20944/preprints202310.1227.v1

organizations are still not taking advantage of asset data to contextualize vulnerability risk, as they lack context to calculate vulnerability risk."

The assets can vary according to the business dynamics, the environment the business is operating in, and the personnel responsible for doing the assessment. The segregation of duties approach engenders an objective assessment of IT asset values. This is an element of the security culture framework (SCM), as set out by Georgiadou et al. [19] (p.3), which combines both "external" human factors and "internal" individual notions, at two levels: the organizational level and the individual level. The organizational level encompasses factors related to an organization's security infrastructure, operations, policies, and procedures. The individual level focuses on the attributes and characteristics of employees that directly impact their security attitudes and behaviors. Each level is further divided into different dimensions. The SCM model thus distinguishes between the organizational and individual levels, each consisting of multiple dimensions that collectively contribute to a comprehensive understanding and evaluation of an organization's security culture.

Information security is also closely related to IT governance. The COBIT (Control Objectives for Information and Related Technologies) framework, which was created in 1996 by the Information Systems Audit and Control Association (ISACA), aims to ensure that IT investments and activities align with strategic objectives. COBIT 2019 [20] is the latest version of the framework and is used in this study. It involves establishing decision-making structures, defining accountability, and setting policies and guidelines for managing IT resources and risks. It provides guidelines and best practices for organizations to ensure effective control and governance over their IT processes, and mitigate IT-related risks.

A risk assessment of IT assets will normally entail the identification of vulnerabilities, threats, and asset values. In this context, the Unified Modeling Language (UML) can provide a useful communications medium for stakeholders to discuss and collaborate effectively during risk assessment. UML uses "elements" and associates them in different ways to form diagrams that represent static, or structural aspects of a system, and behavioural diagrams, which capture the dynamic aspects of a system. A number of previous studies have used UML in risk management research [21]. The class diagram is the most commonly used UML diagram, and features in several other risk management frameworks using UML [22,23].

Given the issues raised in the above discussion, this study addresses the following research questions (RQs):

1. How can subjectivity in assessing IT asset values be addressed, using the segregation of duties approach?
2. Can UML be used to design a flexible risk management system for valuing IT assets in organisations?

3. Research Method and Conceptual Framework

The research method is based on the development of a conceptual framework derived from the extant literature, its application in a systems design using UML, and validation of that design via a survey of 16 experts in the field of study. The research adopts a pragmatic philosophy, and methods are qualitative and inductive. According to Miles and Huberman [24], a conceptual framework "lays out the key factors, constructs, or variables, and presumes relationships among them" (p. 440). Loaiza et al. [25] suggest that the conceptual framework is "a grounded theory technique" and that it "allows researchers to make comparisons and organize ideas. It not only gathers concepts, but also integrates them into one single structure. The goal is to find factors, attributes, variables, behaviour, processes, and so on that describe the new concept" (p.7). According to Jabareen [26] (p.52), "building a conceptual framework from existent multidisciplinary literature is a process of theorization, which uses grounded theory methodology rather than a description of the data and the targeted phenomenon". Conceptual frameworks connect several concepts in a network to investigate a phenomenon [27].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 October 2023 doi:10.20944/preprints202310.1227.v1

The conceptual framework for this study (Figure 2) combines elements of SCM and COBIT 2019. It uses the dimensions of SCM [19] at two levels – organisational and individual. At the organizational level, these dimensions are:

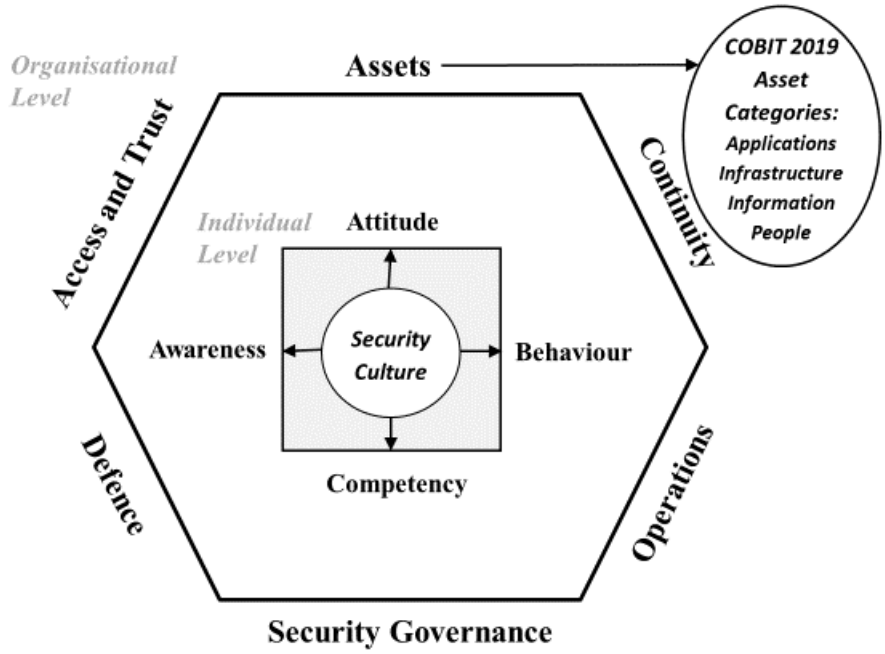

Figure 2. The conceptual framework (incorporating COBIT 19 asset categories and the dimensions of the Security Culture Model).

Assets: People, buildings, machines, systems, and information assets. This dimension also includes policies that enforce different levels of confidentiality, availability, and integrity controls. More specifically, the four COBIT 2019 categories (applications, information, infrastructure, and people) are adopted here.

Continuity: Aims to ensure the continuity of operations, services, and production for the organization at predetermined levels. It also safeguards the reputation and interests of key stakeholders in the event of disruptive incidents.

Access and Trust: Focuses on appropriate access to resources across the organization, clarifying different roles and permissions. It also addresses interactions with third-party entities such as suppliers, customers, and authorities.

Operations: Involves the administration of business practices to achieve the highest level of efficiency, while considering security aspects that protect the organization's final results.

Defense: Emphasizes the importance of planned acquisition and proper configuration of technical assets necessary for the improvement and efficient operation of information security.

Security Governance: Encompasses measures taken to effectively plan, manage, and improve information security within the organization.

The individual level dimensions are:

Attitude: Examines employees' feelings and beliefs towards security protocols and issues.

Awareness: Evaluates employees' understanding, knowledge, and awareness of security issues and activities.

Behaviour: Studies the security-conscious behaviour displayed by individuals in their workplace on a day-to-day basis.

Competency: Assesses employees' abilities, skills, knowledge, and expertise that enable them to adhere to the organization's security policies and procedures.

The conceptual framework also embodies principles of the COBIT 2019 framework for IT governance. The Assets dimension is further classified under four categories; applications,

 doi:10.20944/preprints202310.1227.v1

information, infrastructure, and people, as in COBIT 2019, in which, the "build, acquire, implement" (BAI) domain focuses on defining, acquiring, and implementing IT solutions while integrating them into business processes [20]. "Applications" refers to the automated user systems and manual procedures that process the information. "Information" is the data, in all its forms, input, processed, and output by the information systems in whatever form is used by the business. "Infrastructure" is the technology and facilities (i.e., hardware, operating systems, database management systems, networking, multimedia, and the environment that houses and supports them) that enable the processing of the application. "People" are the personnel required for IT governance including staff concerned with acquisition and implementation of IT resources.

In summary, a conceptual framework was developed to act as a basis for systems design. To engender an objective assessment of IT asset values, the segregation of duties approach was incorporated into the systems design allowing multiple perspectives on IT asset values and other variables. In addition, and in line with best practice, the system accommodates the IT management asset categories from the widely used COBIT 2019 BAI domain.

To validate the systems design, sixteen professionals working in related fields were asked to complete a simple survey which was emailed to them, along with detail of the system design, in September 2023. This was facilitated with the support of the ISACA Istanbul Chapter, with which the authors have established contacts. The survey was in the form of 8 statements with which respondents were asked to state their agreement or disagreement on a 5-point Likert scale. The online survey respondents are a diverse group of highly experienced IT professionals with expertise in IT governance, information security, audit and IT risk assessment. They come from both the public and private sectors and have a wide range of experience levels, with the majority having careers spanning between 10 to 20 years (Table 1). This diversity of backgrounds and experience allowed them collectively to offer a valuable perspective on the assessment of the system's design and security alignment. The questions were relatively simple and designed to provide some indications from practitioners of relevance to the RQs. Results are discussed in section 4 below.

Table 1. Roles of Survey Respondents.

Senior IT Auditor/Consultant with 30 years experience
Senior IT Auditor/Director at major international consultancy with 20 years experience
Information Technology Audit Manager in a Bank with 10 years experience
Executive at IT Security, Risk and Compliance Department with 15 years experience
Cyber Security Consultant at major international consultancy with 3 years experience
Manager at major international consultancy with 13 years experience
Information Security Assistant Manager - CISO at major international insurance company
Head of IT Audit at a leading Turkish banking group
Head of IT Audit in both public and private sector organisations
Chief Information Security Officer at Turkish financial institution with 20 years experience
Head of Internal Audit in Finance Bank in Turkey with 5 years experience
Senior Cybersecurity expert with 15 years experience
Director, IS Audit Leader, major international consultancy with 15 years experience
IT Manager and Auditor roles with 20 years experience
Director, IS Audit Leader in several companies with 20 years experience
IT Security and Audit expert in a University with 10 years experience

4. Results: System Design and Operation

4.1. System Design

The proposed asset-based risk analysis system builds upon the conceptual framework and employs segregation of duties principles to increase the accuracy in human-dependent value assignment, and is aligned with ISO 27001 standards. Figure 3 illustrates the class diagram for the system, accommodating the six organisational level dimensions of the SCM (Assets, Continuity, Access and Trust, Operations, Defense, and Security Governance) and COBIT categories.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 October 2023 doi:10.20944/preprints202310.1227.v1

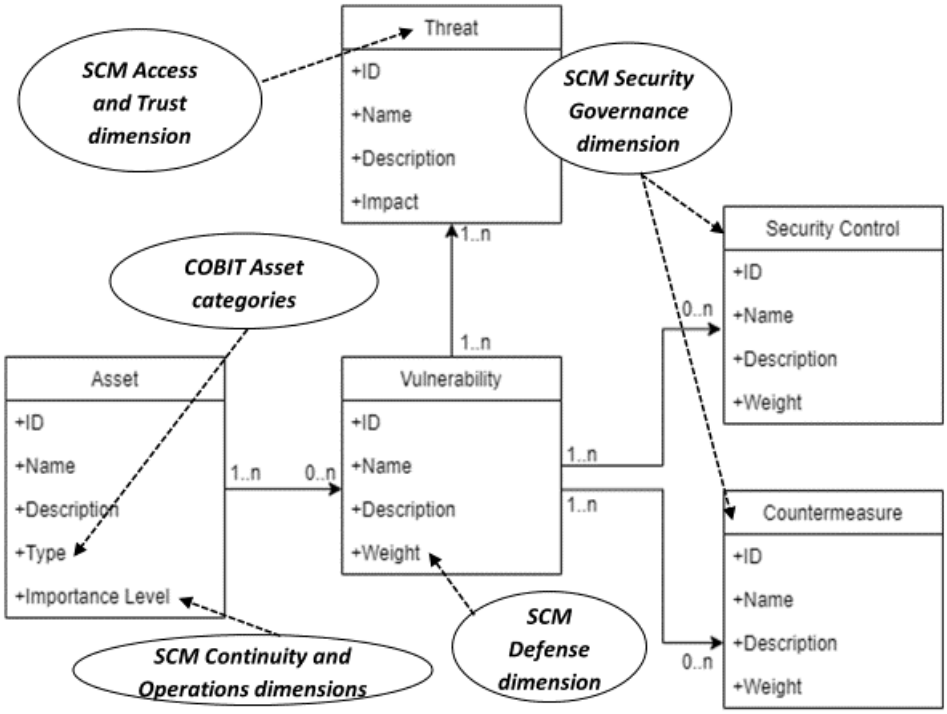

Figure 3. Object classes and relationship to SCM dimensions.

More specifically, the system design comprises five interrelated object classes. The Asset object class contains ID, name and description, but also "type" and "importance level" for each asset. "Type" is the asset categorization taken from the COBIT 2019 Asset Management process [28]. "Importance level" considers the Continuity and Operations SCM dimensions. (Asset ID will be numerical and will be auto-generated rather than user-given). "Importance level" is a number that ranges from 0 to 10 needed for impact analysis, 0 indicating no impact and 10 indicating serious damages to business operations if something happened to that particular asset. In qualitative risk assessment, professionals often prefer to assign high, medium and low importance levels. However, the proposed system requires numeric data to perform risk calculations. For this reason, the numerical priority level ranges can be classified as Low (0-4), Medium (5-7), and High (8-10) as default values.

The Vulnerability object is related to all four other object classes in the system (Asset, Threat, Security Control, and Countermeasure classes), which ensures that any vulnerability is associated with at least one asset in the system, and every threat, security control, and countermeasure are related to at least one vulnerability. It has ID, name, description, and weight attributes. The weight attribute is related to the SCM Defense parameter. For example, if low network security (vulnerability) exists, a hacker attack (threat) can be associated with it. Weight, like the asset priority level, is a numerical number that ranges from 0 to 10 that is used to help calculate the severity of exploitation of this vulnerability to the asset, 0 meaning no impact and 10 meaning serious damages to the asset.

The Threat object class considers the SCM Access and Trust dimension, which focuses on appropriate access to assets across the organisation, clarifying different roles and permissions. It also addresses interactions with third-party entities such as suppliers, customers, and authorities which can be threat sources. The Threat object class, similar to the previous classes discussed, has ID, Name, description, and impact attributes. Threat objects are associated with Vulnerability objects.

The Countermeasure and Security Control object classes consider the SCM Security Governance dimension. The Countermeasure object has ID, name, description and weight attributes. The weight attribute has a numerical value which is subtracted from the calculated risk to find the final risk. Similarly, the Security Control object has ID, name, description, and weight attributes. These security controls are supplied by the organisation which will reflect the organisation's preferences as included

 doi:10.20944/preprints202310.1227.v1

in the ISO 27001 information security management system standard [14]. Some organizations might want to have certain controls involved that will seek to minimize a certain group of vulnerabilities, while others might find such minimisation not to be cost-effective and therefore issue a low weight score to the system to let it prioritise the risks accordingly.

The flow of the system is depicted in the activity diagram (Figure 4). It assumes the existence of a "risk management department" in the organisation. This may exist in several guises and may be located in the organisation's finance or legal department, or be part of the company secretariat. The system assumes four different types of user:

Non-risk department employee: They are typically staff in marketing, sales, administration, customer service, or other department-specific functions. They are experts in carrying out asset-related tasks in their job roles, and thus can make a valid contribution to assessing asset values and risks.

Non-risk department manager: These are managers who oversee departments or units within the organization but are not part of the dedicated risk management department. They have some involvement in risk-related decisions for determining asset values by consulting with non-risk department employees in their department. For example, a sales manager supervising a team of sales representatives or a department head overseeing a specific area like HR or finance.

Risk department specialist: They are individuals who work directly in the organization's risk management department. They confer with non-risk department managers for asset values.

Risk committee: The risk committee is likely to be made up of senior managers, some at Board level, charged with overseeing strategic risk management and related policies. Members will come from various departments or areas of expertise, responsible for managing and making decisions related to risk management strategies and policies, and providing guidance to the organization.

The input from different users fulfilling different roles within the organisation helps improve the accuracy in value assignment in different parts of the system. The system starts with asset identification and data entry. It is assumed that a prior study on departmental assets has been conducted by the departments of the company separately. End-users are believed to be the most competent in evaluating the assets they use. The IT department plays a crucial role in the valuation assessment due to its control over key IT assets like network infrastructure, computers and servers. However, a separate risk department, independent of IT, assesses risks across the entire organization, including those related to finance, operations, legal matters, compliance, strategy, and reputation. These user departments require various software and hardware assets to support their business processes in a digitalised enterprise environment. As a result, the approach set out here not only directly addresses IT-related risks, but also indirectly covers a wide range of risk types in different departments that are associated with the use of IT assets to support business processes. Whilst the focus is essentially on Information Security as depicted in Kosutic's model (Figure 1), the incorporation of the SCM dimensions (Operations, Continuity, Governance) into the system design and operation (as shown in Figure 3) means that wider risks are considered in the context of their impact on the IT assets of the organisation.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 October 2023 doi:10.20944/preprints202310.1227.v1

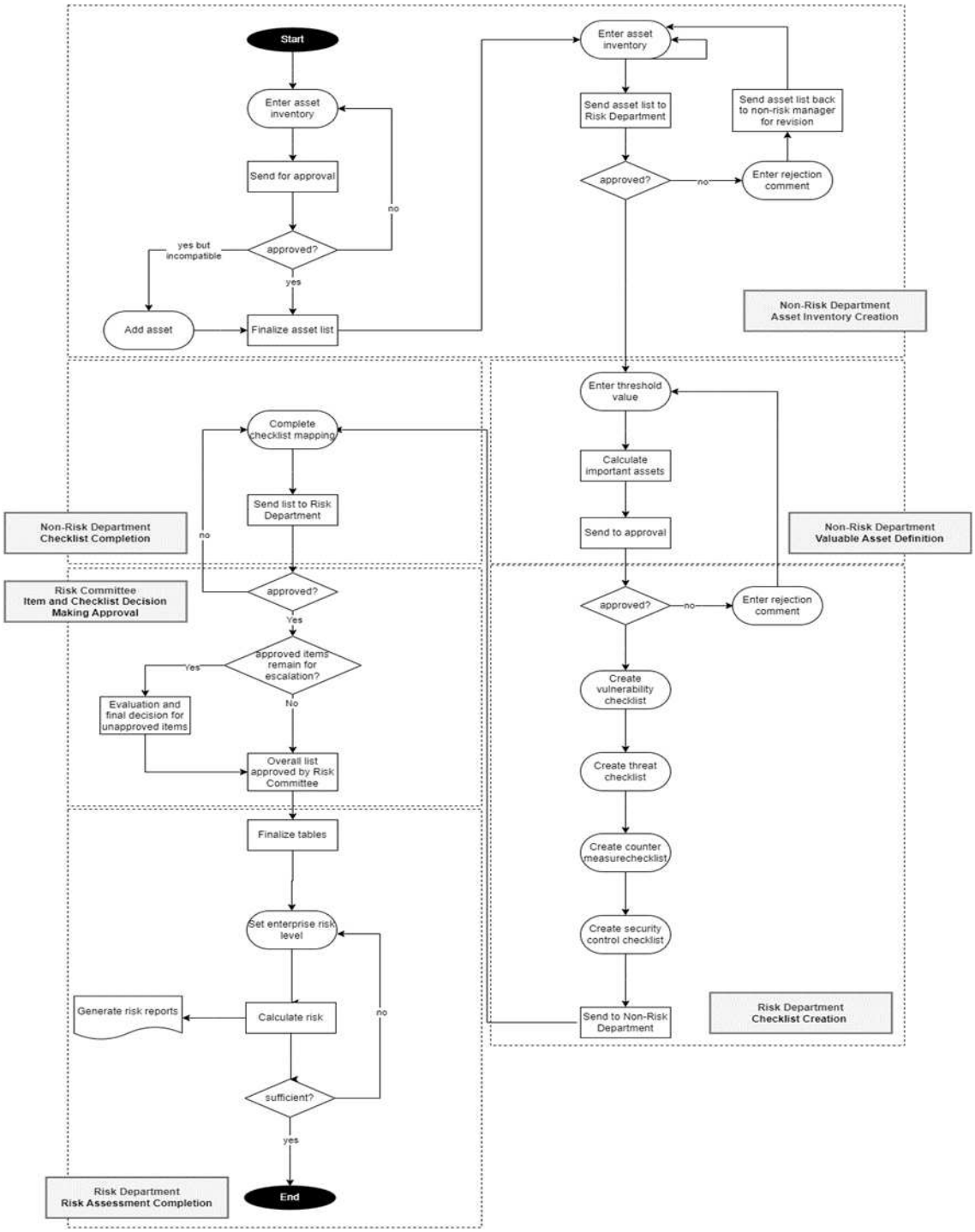

Figure 4. Activity diagram representing system operation.

4.2. System Operation

The non-risk department employees enter the assets one by one, using existing asset inventory records as appropriate, and the system sends the complete list to the relevant non-risk department manager. The non-risk department manager checks the lists and may approve all, approve some, update or erase some of the assets. After the asset list is completed, the non-risk department manager enters the values to the assets and sends the list to the risk department specialist, who evaluates the asset list and the asset values and may approve all or approve some. If there are some unapproved assets that remain, the risk department specialist enters comments on what should be changed and sends them to the non-risk department manager to review. This process continues until all of the

 doi:10.20944/preprints202310.1227.v1

assets have been approved by the risk department specialist. In this way, an asset inventory is prepared for the department.

IT assets are categorised and prioritised based on their importance and criticality. To ensure objectivity in this prioritization process, the non-risk department manager seeks guidance from a risk department specialist. The non-risk department manager sets specific threshold values for the priority categorization, allowing room for experimentation with different levels and a review of the asset lists. Once the non-risk department manager determines the threshold, it is then submitted for approval by the risk department specialist.

When all of the asset lists are prepared, the risk department specialist creates vulnerability, threat, security-control, and countermeasure checklists for each department separately. The risk department creates a vulnerability checklist first because threats can affect the business only if the related vulnerabilities are exploited. Different threats, vulnerabilities, security controls, and countermeasures are saved to the system library for reuse. Again, it is assumed that the risk department conducts prior research on the various risk factors which may impact the assets of the business, and their controls and/or countermeasures. The completed checklists are sent to the non-risk department employee to review and also to enter the vulnerability weight for each of the marked vulnerabilities. The non-risk department employee can also add threats, vulnerabilities, security controls, and countermeasures if necessary, and send the completed lists to the risk department after manager approval.

The risk department specialist then checks the additions made by the non-risk department employee. The risk department specialist may approve all of the additions or approve some of the additions. If some unapproved things remain, the risk department specialist sends the unapproved lists back to the non-risk department employee. After discussions between the non-risk department manager and risk department specialist, some items in the list may remain unapproved. Such items will be escalated to the risk committee for their evaluation and final decision. In addition, the overall list needs to be approved by the risk committee. When all of the lists are approved by the risk committee, the proposed system finalises the asset, threat, vulnerability, countermeasure, and security control tables. In this manner, the subjectivity of qualitative risk assessment is mitigated, since the inaccurate opinion of a solitary user is not utilized to determine asset values. Moreover, individual factors such as Attitude, Awareness, Behavior, and Competency in SCM are duly considered.

The flow continues with the risk department specialist setting the company risk level. The risk level differs from sector to sector and from company to company. The risk level is the decisive factor which determines which risks will be disregarded, and which ones will be regarded as significant. According to the risk level, the system will calculate the company risks and produce various risk-related reports. With this information, the risk department can get a top-line view of the company's IT risk position, and its breakdown at departmental level, and take strategic decisions accordingly. If the risk department wants to see what-if scenarios by changing their risk appetite levels, they can re-set the risk level to a higher or lower level, and the system will automatically re-calculate the risks.

In this calculation, the asset priority level is utilsed, as well as the severity of the threat (impact) and the weight of vulnerabilities. These factors are combined to derive a risk severity score for a specific asset. Next, the system calculates the probabilities of each threat happening depending on prior data. The system gathers past data regarding how often these threats were seen, and calculates the probability of a risk.

5. Validation and Discussion

The system outlined above is an example of how the principles embodied in the conceptual framework can be mapped into an operational system. It is but one example, and will not suit all environments, and many other options are possible. As noted in section 3 above, 16 practitioners were contacted to gain some feedback on the value of the proposed design. The 8 statements adopted a positive position as regards the proposed system, and overall, respondents were very supportive of these statements, with the vast majority of responses either strongly agreeing or agreeing with

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 19 October 2023 doi:10.20944/preprints202310.1227.v1

them (Table 2). The risk assessment method embodied in the proposed system was viewed as generally supportive of business sustainability (Statement 1), and all but one respondent considered it would minimise subjectivity in risk and IT value assessment (Statement 5). Other benefits relating to the utilised knowledge base, the value of different perspectives and the raising of information security awareness were also supported (Statements 6, 7 and 8).

Table 2. Survey responses regarding value of the proposed risk assessment method.

No.	Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1	The risk assessment method is beneficial for business sustainability	8	8	0	0	0
2	The risk assessment method is suitable for small-scale businesses (<50 staff).	3	8	3	2	0
3	The risk assessment method is suitable for medium-sized businesses (50-250 staff).	3	12	1	0	0
4	The assessment method is suitable for large businesses (>250 staff).	6	10	0	0	0
5	The risk assessment method helps mimimise subjectivity.	1	12	3	0	0
6	The risk assessment method benefits from the involvement of individuals who have an in-depth understanding of the specific details related to assets.	8	7	1	0	0
7	The risk assessment method benefits from a combination of high-level management guidance and operational perspectives.	8	8	0	0	0
8	The risk assessment method increases employees' information security awareness.	9	7	0	0	0
	TOTALS	46	72	8	2	0

When asked to comment on the suitability of the method for different size of company, respondents were more negative as regards smaller companies, probably reflecting the fact that such companies may not have the resources for a risk management function and risk committee (Statements 2,3,4).

There are other issues that the proposed systems design raises that are worthy of discussion. The system is based on a flow of tasks that make the risk calculation process relatively simple and allows flexibility in setting up the system variables. The weights and the impacts are illustrative, allowing organisations to customise the system according to their IT and operational environments.

The conceptual framework upon which the system design is based, integrates SCM and COBIT 2019 approaches, facilitating a more holistic view of the IT risk assessment process. This is accomplished by conducting a thorough and unbiased assessment of IT assets, ensuring that the evaluation remains unaffected by potential inaccuracies or misjudgments, stemming from individual viewpoints that may not be entirely correct or accurate. Furthermore, it allows a detailed objective assessment of assets values in line with COBIT 2019 through UML modelling, this being the first instance of such an approach. The system can be seen to reduce the individual assessment of risks by integrating a segregation of duties, while building upon the assumption that the people working at the risk department are competent and are aware of current technology trends. Although human

 doi:10.20944/preprints202310.1227.v1

error and/or poor communication may lead to inaccurate data input to the system, in general the segregation of duties ensures a high degree of objectivity and cross-checking that minimises the risk of human error or personal differences of risk perception.

6. Conclusions

The conceptual framework and system design discussed in this article responds to the two research questions set out in section 2: how can subjectivity in assessing IT asset values be addressed, using the segregation of duties approach (RQ1)? and: can UML be used to design a flexible risk management system for valuing IT assets in organisations (RQ2)? The system is an illustration of how UML can be used in the design of a system which integrates a segregation of duties approach to reduce the subjectivity of IT asset and risk valuations. It helps to gather and improve company risk knowledge while engendering better-informed decision making. This study highlights the value of using UML in an information security domain, the flexibility of UML allowing customization of the risk management system according to the size and specific needs of organizations. The weights and the impacts allow for flexibility in conducting appropriate risk analyses in different organisations, creating a more customized risk assessment.

The research presented here has its limitations. The method of assessment of risk and related aspects makes certain assumptions that will not always apply in all organisations. Indeed, the questionnaire feedback indicated that smaller businesses of less than 50 staff may find it difficult to provide the resources for the risk professionals required to run the proposed system, and that this approach may better suit the medium and larger size companies where more resources are available for this type of activity. The scope of the study is also limited to a certain number of user types, and future research could usefully enhance the scope of the system by incorporating more user types, as well as additional human error factors within the types of vulnerability, for example.

To some, in this age of digital transformation, with the metaverse and quantum computer on the IT horizon [29], the system outlined here may appear simplistic and outdated in approach. It is maintained here that this is not the case. Rather, it reflects the dearth of proven approaches to IT-asset valuation and risk assessment, as evidenced in the growing focus on this issue in the recent literature. As Nost et al. [18] (para. 8) note "to remediate vulnerabilities and security gaps and get a more accurate view of their overall security posture, firms must understand the criticality of business processes, which assets support them, and what compensating controls and security tools are on those assets". The approach set out here is a valid framework that can be built upon and developed by other researchers and practitioners, and is amenable to incorporation of digital technology access and support (mobile, analytics, cloud).

There are also wider dimensions to this problematic that warrant further research. The implications of integrated supply chains, where companies have access to each other's systems and technologies [30], introduces further complexity that merits research and assessment. Equally, the provision of IT services and infrastructure through outsourcing moves the management of risk in large part to the third-party provider, but there remain some security risks in such arrangements that need addressing and managing via service-level agreements. As recently noted by ISC2 [31] (p.7), a leading member association for cybersecurity professionals, "having visibility and a solid understanding of what must be protected, what access should be restricted, the available control mechanisms and how these may be abused is the foundation of all security controls. The professional should be able to apply the principles of confidentiality, integrity, availability, and privacy against these information assets". It is hoped that the further development and application of systems like that outlined here can make a small contribution to this endeavour.

Author Contributions: Conceptualization, B.M., S.D., E.T., M.M., and M.W.; methodology, B.M., S.D., E.T., M.M., and M.W.; software, B.M., S.D., E.T., and M.M.; validation, B.M. and M.W; formal analysis, B.M., S.D., E.T., and M.M.; investigation, B.M., S.D., E.T., and M.M.; resources B.M., S.D., E.T., and M.M.; writing—original draft preparation, B.M., S.D., M.M. and M.W.; writing—review and editing, B.M. and M.W.; visualization, B.M., S.D., E.T., M.M., and M.W.; supervision, B.M.; project administration, B.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Survey data was provided on the basis of anonymity and thus further detail is unavailable in the public domain.

Acknowledgments: The authors express their gratitude to the Information Systems Audit and Control Association (ISACA) Istanbul Chapter for their valuable collaboration in conducting the survey for this study.

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

References

1. Zwikael, O.; Ahn, M. The effectiveness of risk management: an analysis of project risk planning across industries and countries. *Risk Analysis* **2011**, *31*(1), 25-37.
2. Zayed, T.; Amer, M.; Pan, J. Assessing risk and uncertainty inherent in Chinese highway projects using AHP. *International Journal of Project Management* **2008** *26*(4), 408-419. doi: 10.1016/j.ijproman.2007.05.012.
3. Nost, E.; Burn, J. CISA Releases Directives on Asset Discovery and Vulnerability Enumeration. 2022. Forrester. Available online: https://www.forrester.com/blogs/cisa-releases-directives-on-asset-discovery-and-vulnerability-enumeration/ (accessed on 4 October 2023).
4. Rapid7. Evaluating Vulnerability Assessment Solutions. No date. Available online: https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-vulnerability-assessment-buyers-guide.pdf (accessed 9 October 2023).
5. Irizar, J.; Wynn, M. Development and Application of a New Maturity Model for Risk Management in the Automotive Industry. In Global Risk and Contingency Management Research in Times of Crisis; N. Vajjhala; K. Strang, Eds.; IGI Global: Hershey, USA. 2022; pp. 29-52. https://doi.org/10.4018/978-1-6684-5279-0.ch003
6. Carleton, J.; Krishnamoorthi, S. Digital Risk: The Security Challenge Beyond Your Perimeter. Frost & Sullivan White Paper. 2019. Frost & Sullivan: Santa Clara, CA, USA.
7. Karlsson, F.; Hedström, K.; Goldkuhl, G. Practice-based discourse analysis of information security policies. *Computers & Security* **2017**, *67*, 267-279.
8. Awati, R. Segregation of Duties (SoD). 2023. TechTarget/Whatis.com. Available online: https://www.techtarget.com/whatis/definition/segregation-of-duties-SoD (accessed on 8 August 2023).
9. Hedström, K.; Kolkowska, E.; Karlsson, F.; Allen, J. P. Value conflicts for information security management. *The Journal of Strategic Information Systems* **2011** *20*(4), 373-384.
10. Crespo-Martinez, P. E. Selecting the Business Information Security Officer with ECU@ Risk and the Critical Role Model. In International Conference on Applied Human Factors and Ergonomics. Springer: Cham, Switzerland; 2019; pp 368-377.
11. Middleton, J. Capita cyber-attack: 90 organisations report data breaches. *The Guardian*. 30 May 2023 Available online: https://www.theguardian.com/business/2023/may/30/capita-cyber-attack-data-breaches-ico (accessed on 20 July 2023).
12. Cram, W. A.; Proudfoot, J. G.; D'arcy, J. Organizational information security policies: a review and research framework. *European Journal of Information Systems*, **2017** *26*(6), 605-641.
13. Safa, N. S.; Maple, C.; Furnell, S.; Azad, M. A.; Perera, C.; Dabbagh, M.; Sookhak, M. Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems* **2019,** *97*, 587-597.
14. ISO/IEC. ISO/IEC 27001 Information technology — Security techniques - Information security management systems — Requirements. 2013. Available online: http://www.itref.ir/uploads/editor/42890b.pdf (accessed on 23 August 2023)
15. Kosutic, D. ISO 31000 and ISO 27001 – How are they related? 2022. Available online: https://advisera.com/27001academy/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/#:~:text=In%20clause%206.1.-,3%2C%20ISO%2027001%20notes%20that%20information%20security%20management%20in%20ISO,already%20compliant%20with%20ISO%2031000 (accessed on 23 August 2023).
16. Irwin, L. Conducting an asset-based risk assessment in ISO 27001. 2022. Vigilant. Available online: https://www.vigilantsoftware.co.uk/blog/conducting-an-asset-based-risk-assessment-in-iso-270012013 (accessed on 24 August 2023).
17. Weil, T. Risk assessment methods for cloud computing platforms. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). Vol. 1., IEEE; 2019; pp. 545-547.
18. Nost, E.; Maxim, M.; Bell, K.; Worthington, J.; DiCicco, H. The State of Vulnerability Risk Management 2023. 2023. Forrester Report. Available online: https://reprints2.forrester.com/#/assets/2/1730/RES179028/report (accessed on 22 August 2023).

19. Georgiadou, A.; Mouzakitis, S.; Bounas, K.; Askounis, D. A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems* **2020,** *62*(3), 452-462. https://doi.org/10.1080/08874417.2020.1845583
20. Cristopher A. Employing COBIT 2019 for Enterprise Governance Strategy. 2019 Available online: https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy (accessed on 11 September 2023).
21. Mishra, S.K.; Mishra, A; Mohapatra, D.P. Risk Analysis of a system at design level using UML Diagrams. 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI). Available online: https://ieeexplore.ieee.org/document/6637170 (accessed on 9 August 2023).
22. Alamri, Q.; Ali, M. A.; Tahir, N. M. Information Technology Risk Management in Oman. In 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA). IEEE; 2020; pp 308-312.
23. Martin-Guillerez, D.; Guiochet, J.; Powell, D.; Zanon, C. A UML-based method for risk analysis of human-robot interactions. In Proceedings of the 2nd International Workshop on Software Engineering for Resilient Systems. 2010; pp. 32-41.
24. Miles, M. B.; Huberman, A. M. *Qualitative data analysis: An expanded source book*, 2nd ed. Sage: Newbury Park, CA, USA; 1994.
25. Loaiza, J.H.; Cloutier, R.J.; Lippert, K. Proposing a Small-Scale Digital Twin Implementation Framework for Manufacturing from a Systems Perspective. *Systems* **2023**, *11*, *41*, 1-24. https://doi.org/10.3390/systems11010041.
26. Jabareen, Y. Building a Conceptual Framework: Philosophy, Definitions, and Procedure. *Int. J. Qual. Methods* **2009**, *8*, 49–62.
27. Levering, B. Concept Analysis as Empirical Method. *Int. J. Qual. Methods* **2002**, *1*, 35–48.
28. Harisaiprasad, K. *COBIT 2019 and COBIT 5 Comparison*. 2020. ISACA. Available online: https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison (accessed on 12 October 2023).
29. Wynn, M.; Jones, P. New technology deployment and corporate responsibilities in the metaverse. *Knowledge* **2023**, *3*(4), 543-556. doi:10.3390/knowledge3040035
30. Nightingale, C. Managing cyber risk through integrated supply chains. *Computer Weekly*. September 21, 2021. Available online: https://www.computerweekly.com/opinion/Managing-cyber-risk-through-integrated-supply-chains?utm_campaign=20211229_ERU+Transmission+for+12%2F29%2F2021+%28UserUniverse%3A+364164%29&utm_medium=EM&utm_source=ERU&src=8907352&asrc=EM_ERU_198647440&utm_content=eru-rd2-rcpC (accessed on 9 October 2023).
31. ISC2. 9 traits you need to succeed as a cybersecurity leader. 2020. Available online: https://media.bitpipe.com/io_16x/io_167060/item_2670924/Res%20ID_%201665550744_355_%209-Traits-You-Need-To-Succeed-As-A-Cybersecurity-Leader-Whitepaper-RB.pdf (accessed on 9 October 2023).