information

MDPI

Article

IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture

Bilgin Metin [1], Sefa Duran [2], Eda Telli [3], Meltem Mutlutürk [1] and Martin Wynn [4,*]

[1] Department of Management Information Systems, Bogazici University, Hisar Campus, Bebek, Istanbul 34342, Turkey; bilgin.metin@boun.edu.tr (B.M.); meltem.mutluturk@boun.edu.tr (M.M.)
[2] Independent Researchers, 2628 TJ Delft, The Netherlands; m.sefaduran@gmail.com
[3] Independent Researchers, Istanbul 34660, Turkey; eda.yamamoto@tages.biz
[4] The School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL50 2RH, UK
* Correspondence: mwynn@glos.ac.uk

Abstract: In today's technology-centric business environment, where organizations encounter numerous cyber threats, effective IT risk management is crucial. An objective risk assessment—based on information relating to business requirements, human elements, and the security culture within an organisation—can provide a sound basis for informed decision making, effective risk prioritisation, and the implementation of suitable security measures. This paper focuses on asset valuation, supply chain risk, and enhanced objectivity—via a "segregation of duties" approach—to extend and apply the capabilities of an established security culture framework. The resultant system design aims at mitigating subjectivity in IT risk assessments, thereby diminishing personal biases and presumptions to provide a more transparent and accurate understanding of the real risks involved. Survey responses from 16 practitioners working in the private and public sectors confirmed the validity of the approach but suggest it may be more workable in larger organisations where resources allow dedicated risk professionals to operate. This research contributes to the literature on IT and cyber risk management and provides new perspectives on the need to improve objectivity in asset valuation and risk assessment.

Keywords: risk assessment; asset value; information security; risk management; objective risk assessment; segregation of duties; security culture framework; COBIT 2019; international standards; cybersecurity; supply chain security

Citation: Metin, B.; Duran, S.; Telli, E.; Mutlutürk, M.; Wynn, M. IT Risk Management: Towards a System for Enhancing Objectivity in Asset Valuation That Engenders a Security Culture. *Information* **2024**, *15*, 55. https://doi.org/10.3390/info15010055

Academic Editor: Rúben Pereira

Received: 20 December 2023
Revised: 12 January 2024
Accepted: 15 January 2024
Published: 17 January 2024

1. Introduction

IT risk management has been a fundamental discipline in most industry sectors for several decades, but its significance has come to the fore in recent years in the context of cybersecurity and the rapid growth of the associated risks to organisations and society at large [1]. Within IT's functions, risk management may be an element within a wider disaster recovery plan, which may also be viewed as part of a business continuity plan at a corporate level. However, although risk management features in a number of industry standard methodologies, there is no universally agreed method for managing IT-related 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].

Practically all company activities come with a particular risk associated with them. While 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 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 prioritise 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 [3]. These may help companies to put 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 continuity 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 one of the main contributory causes. Carelton and Krishnamoorthi [4] (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" and concluded that "organizations are also struggling to stay ahead of cybercriminals 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 prioritisation, and effective decision making [5], which can help address the concern of subjectivity in the assessment of risk. In this research, a "segregation of duties" approach was 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 [6] (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 claims 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 paper addresses the need for methods that enhance objectivity in IT risk management practices. This has been the subject of research in other fields involving risk, notably in project management [7], and whilst the criticality of this subject in the context of IT security is evidenced in recent publications [8–10], this is one of the first studies to address the philosophical dilemma in IT risk assessment regarding the subject–object relationship. It points out the challenge of maintaining objectivity due to the inherent link between an asset and its owner. While stressing the importance of unbiased and complete information in assessments, the study also recognises the crucial role of human factors in cybersecurity. This situation presents a paradox: the need for impartial assessments that still consider the human aspects of asset ownership and risk. An improved security culture framework is put forward that incorporates a "segregation of duties" approach to reduce subjectivity and personal biases in risk assessments. This approach aims to provide a clearer and more accurate understanding of actual risks. The paper discusses the design of a system based upon this model and validates its effectiveness through a survey of 16 practitioners from both private and public sectors. Risks from supply chain attacks and asset valuation with enhanced objectivity are also incorporated within the conceptual model. By targeting this gap in the literature, the research outcomes detailed in this article contribute to the field of IT and cyber risk management, offering new perspectives based upon an eclectic conceptual model for improving objectivity in asset valuation and risk assessment processes. For clarity, the unified modelling language (UML) is used in the system design process.

The paper comprises seven sections. Following this introduction, the research method is outlined. Relevant literature and standards are examined in Section 3, and two research questions are set out. Section 4 then establishes the conceptual model for the system, which

builds upon an established security culture framework. Section 5 outlines the system design and operation, and validation and related issues are discussed in Section 6, including the difficulty of balancing objectivity and subjectivity in IT risk management. The concluding section summarises the findings from the study and discusses limitations and possible future areas of research.

2. Research Method

The study adopted a pragmatic research philosophy, and the methods were qualitative and inductive, including four distinct phases (Figure 1). First, a scoping literature review was undertaken in January–March 2022 to identify key themes and relevant frameworks and standards. This type of review is "best employed when there is limited literature to inform the research question of interest" [11] and can help develop an overall research aim into more specific research questions. This was the case here as the review identified a range of literature sources, standards, and frameworks of relevance to the progression of the overall research aim.

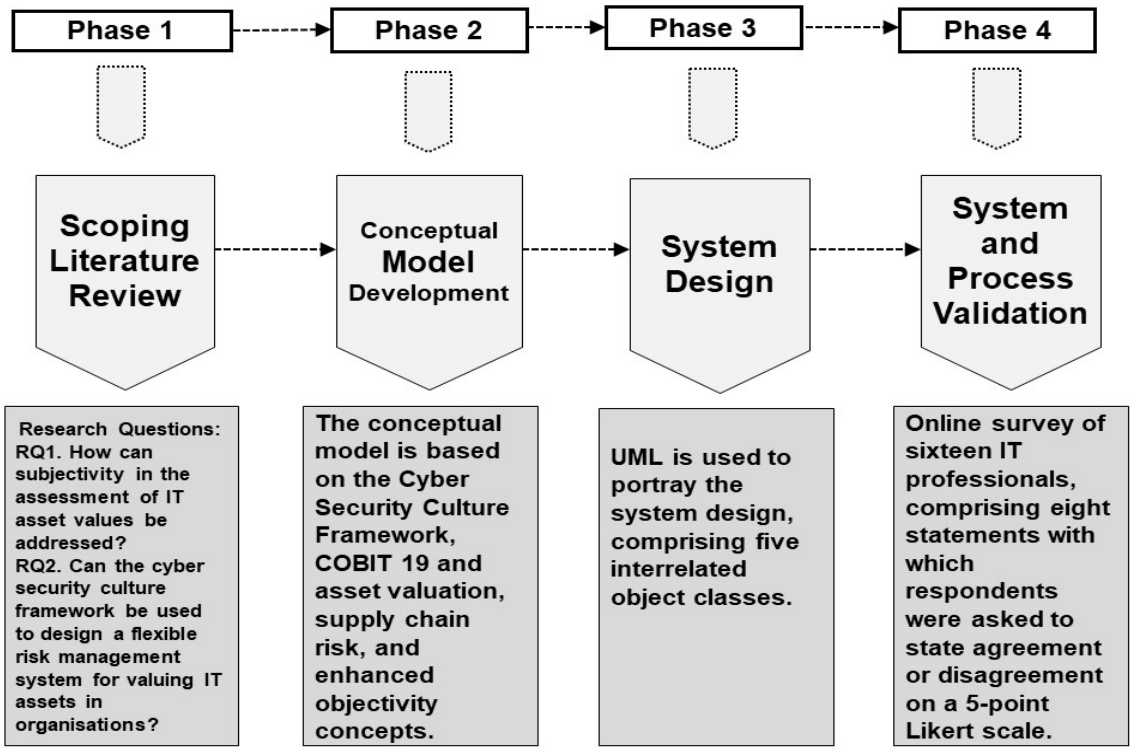

Figure 1. Research method: the four phases.

The literature review was carried out between July and November 2023, employing the Google Scholar search engine. Appropriate search strings were utilised, such as "risk assessment", "asset value", "information security", "security culture", "subjectivity in risk assessment", and combinations of the same. These keywords were carefully chosen to encompass key themes pertinent to the research aim and thereby capture a broad spectrum of relevant literature sources, frameworks, and standards.

As relevant sources were identified, references and relevant quotations were recorded on a spreadsheet, enabling the systematic organisation and evaluation of the literature. The spreadsheet was continuously updated and reorganised to align the source material around the key emergent themes identified in the literature and relevant standards.

The second phase entailed the development of a conceptual model which "lays out the key factors, constructs, or variables, and presumes relationships among them" [12] (p. 440). According to Greca and Moreira [13] (p. 5), a conceptual model can be seen as "an external representation created by researchers, teachers, engineers, etc., that facilitates

the comprehension or the teaching of systems or states of affairs in the world". More specifically, Wand and Weber [14] (p. 363), in the context of information systems, note that conceptual models have several purposes: supporting communication between developers and users, helping analysts understand a domain, and providing input for the design process. Conceptual models can connect several concepts in a network to investigate a phenomenon [15]. The cyber security culture framework put forward by Georgiadou et al. [16] was identified as a valid and appropriate starting point from which to develop the overall conceptual model for the research. Wand and Weber [14] put forward a framework for a systematic approach to conceptual modelling, including a "grammar", a "method", and a "script" (p. 364). Here, a more intuitive approach was pursued, in which the model was anchored on the framework developed by Georgiadou et al. [16], noted above, and other key components from the literature and existing standards were then incorporated, reflecting the interpretivist approach adopted in the research.

In a third phase, the conceptual model was used as the basis for a system design, using the unified modelling language (UML) as the graphic presentation tool. Such graphical presentation of information improves communication and interaction between parties involved in the analysis and facilitates the documentation of risk assessment results and the assumptions on which these results depend. More specifically, UML uses "elements" and associates them in different ways to form diagrams that represent the 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 [17]. The class diagram is the most commonly used UML diagram and features in several other risk management frameworks using UML [18,19].

Finally, the system design and the associated processes were validated via a survey of sixteen experts in the field of study. There are various perspectives on the number of respondents needed for such surveys, but Bertaux [20] argued that fifteen is the smallest acceptable sample size in qualitative research.

The online survey respondents were carefully selected for their extensive experience and diverse backgrounds in IT governance, information security audit, and IT risk assessment. Their collective expertise, spanning both the public and private sectors and ranging from 10 to 20 years of professional experience, provided a comprehensive perspective on the system's design and security alignment. The roles of survey respondents, many of whom work in leading companies in Turkey, are given in Table 1.

Table 1. Roles of survey respondents.

Senior IT auditor/consultant with 30 years' experience
Senior IT auditor/director at a major international consultancy with 20 years' experience
IT 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 a major international consultancy with 3 years' experience
Manager at a major international consultancy with 13 years' experience
Information security assistant manager at a 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 a Turkish financial institution with 20 years' experience
Head of internal audit in a finance bank in Turkey with 5 years' experience
Senior cybersecurity expert with 15 years' experience
Director and IS audit leader at a major international consultancy with 15 years' experience
IT manager and auditor roles with 20 years' experience
Director and IS audit leader in several companies with 20 years' experience
IT security and audit expert in a university with 10 years' experience

The survey itself was designed to be straightforward, easy to respond to, and lacking ambiguity. In this context, Krosnick [21] (p. 95) notes that "an important aspect of validity is that the survey is designed in such a way as to minimise respondent error". The survey took the form of 8 statements with which respondents were asked to state their agreement or disagreement on a 5-point Likert scale. The questions were relatively simple and designed to provide some indications from practitioners of relevance to the RQs. The survey was emailed to them, along with details 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 results are discussed in Section 6 below.

3. Literature, Regulations, and Standards

3.1. Concepts and Methods

Both quantitative and qualitative techniques can be used to assess risk, but many companies lack access to the accurate financial data that are required to use quantitative methods to assess IT asset values. The factor analysis of information risk (FAIR) methodology, for example, helps organisations assess their exposure to cyber risk and quantify it in financial terms. Users are required to feed key data into FAIR's mathematical algorithms, which then "calculate and quantify cyber-risk in terms of probable financial losses" [22] (para. 4). However, the required data input for quantitative assessments—for example, measures such as single loss expectancy, annualised rate of occurrence, and annualised loss expectancy—may not be readily available [23], and other limitations include complexity, limited scope, subjectivity, lack of standardisation, and cost [24]. Many organisations 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 organisation [25]. This has been highlighted by the data breaches and attacks suffered by many organisations in recent years [26], and information security management is being increasingly viewed as an important tool in ensuring organisational continuity [27,28].

Risk analysis is an essential component of an information security management system (ISMS) that 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. CORAS is one of the most cited methodologies in this context [29]. CORAS offers a specialised approach for performing security risk assessments. It includes a tailored language designed for modelling threats and risks, accompanied by comprehensive guidelines. These guidelines detail how to effectively utilise this language for capturing and modelling pertinent information throughout the different phases of the security analysis process [30]. However, qualitative risk assessment involves subjective prioritisation that may lead to inappropriate asset valuations that underpin important decisions regarding information security management.

Risk assessment can be conducted in two ways: scenario-based or asset-based assessment. Scenario-based assessment deals more with the circumstances of the threat [31], but Nost et al. [32] (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, organizations are still not taking advantage of asset data to contextualise vulnerability risk, as they lack context to calculate vulnerability risk." 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 [33]. Vulnerabilities are the weaknesses in corporate software and applications, as well as shortcomings in hardware and infrastructure, which may allow attackers to exploit these vulnerabilities and thereby access and harm the company systems themselves. A threat is the potential of an attacker being able to exploit a vulnerability.

3.2. Asset Valuation

Although there are numerous studies on risk assessment in the literature, only a few focus on determining asset value. Loloei et al. [34], for example, describe a process for business asset valuation that begins with quantifying tangible and intangible assets, which are then converted into qualitative assessments. Subsequently, business process criteria are evaluated in relation to the assets, resulting in the final qualitative valuation of the assets. Tatar and Karabacak [35] introduced a two-step asset valuation technique. The first step involves a top-down approach to identify assets, while the second step employs a bottom-up approach for asset valuation. This method categorises assets into three types—hardware, software, and information—and determines their values based on criteria related to confidentiality, integrity, and availability. Kassa and Cisa [36] introduced a strategy to assess and manage information system assets, emphasizing their confidentiality, integrity, and availability (CIA). They outline a method to identify, record, and sort these assets according to their CIA security objectives and the importance of the data they handle or transfer. Ruan [37] offers a modern approach to evaluating digital assets and managing cyber risks. It diverges from traditional methods by focusing on economic modelling for digital assets. Ekstedt et al. [38] introduce an asset modelling technique for identifying vulnerabilities and potential cyberattack targets within an organisation's IT infrastructure. Few studies, however, calculate asset values by considering both the human factors and business perspectives, while also taking into account traditional approaches to achieve a more accurate risk assessment.

3.3. Third-Party and Supply Chain Cybersecurity

Third-party and supply chain cybersecurity risks are closely related but have distinct characteristics, and understanding the nuances between them is important for effective risk management. Third-party security risks can be mitigated using contractual agreements and access control countermeasures. However, managing supply chain risks often involves ensuring the security of products and services throughout their lifecycle, from design to disposal, which is difficult to control. It includes vetting suppliers' cybersecurity practices, monitoring for threats across the supply chain, and planning for continuity in case of disruptions. Supply chain cybersecurity is now a crucial consideration for organisations across various sizes and industries [39].

In addressing the challenge of assessing security practices in large organisations, particularly when integrating third-party services, Edwards et al. [40] highlighted the limitations of traditional risk assessment methods like audits and questionnaires. These conventional approaches often fail to capture the dynamic nature of third-party security risks, which are exacerbated by the integration of external services involving the sharing of sensitive data and extensive network integration. Their study proposed an innovative approach using external measurements to construct per-organisational "risk vectors", offering a more objective, quantitative, and non-invasive method of assessing these risks. This approach is particularly pertinent in the modern business landscape, where third-party collaborations are common and can inadvertently introduce vulnerabilities, underscoring the need for more effective risk assessment methodologies in organisational security management.

In the realm of cloud computing, the identification and management of third-party security risks are of paramount importance, as highlighted by Youssef [41]. The outsourcing of sensitive data to third-party providers in cloud environments introduces a complex array of security risks. This complexity is compounded by the diverse and numerous security controls inherent in cloud models. Despite the implementation of robust security measures, organisations continue to face challenges in establishing trust in cloud computing, largely attributable to the uncertainty regarding the consequences of these security risks. Traditional risk management frameworks often fail to adequately address the impact of cloud security risks on an organisation's business objectives. Consequently, a focused approach towards identifying and mitigating third-party security risks is crucial for aligning cloud security strategies with organisational goals and objectives.

The research conducted by Dennig et al. [42] on open-source software vulnerabilities in large organisations underscores a broader concept in cybersecurity: the significance of identifying third-party security risks. This study reveals how vulnerabilities in external software components, often integrated into larger systems, pose substantial risks. It highlights the complexity and challenges in effectively detecting and managing these external vulnerabilities. This insight reflects a critical aspect of modern cybersecurity: the need for vigilant assessment and mitigation strategies for third-party security risks, emphasizing their potential impact on the overall security posture of organisations.

Goyal et al. [43] discuss leveraging machine learning to manage risks in complex engagements. They underline the importance of identifying third-party security risks in project management and propose machine learning as a tool to analyse past project data for risk identification. This approach addresses the challenge of managing risks in large organisations where different units often work in silos, thereby emphasizing the significance of a holistic and informed approach to third-party risk management. Hu et al. [44] highlight the criticality of understanding third-party security risks in digital supply chains. Through a data-driven approach, their study reveals how attributes of digital supply chains are significant predictors of enterprise cyber risk, emphasising the necessity for organisations to augment traditional internal cybersecurity assessments with external supply chain insights and highlighting the potential for third-party connections to amplify cyber risks.

In a similar vein, Khani et al. [45] emphasise the crucial role of identifying and mitigating third-party security risks in the realm of web services. In today's interconnected digital environment, organisations increasingly rely on web services to integrate diverse functionalities and create composite services. This integration, while beneficial, introduces significant security vulnerabilities, particularly when involving third-party services. The authors put forward a proactive approach in selecting third-party web services, where the evaluation of potential security vulnerabilities is as critical as assessing performance. They propose the adoption of intrusion-tolerant composite web services tailored to specific functionalities, ensuring that third-party services are not only efficient but also secure. By employing penetration testing tools to assess these vulnerabilities, organisations can significantly reduce the risk of security breaches. Their research highlights the importance of a security-first approach in the selection and integration of third-party web services, underlining the need for rigorous security assessments to safeguard organisational assets and data.

The supply chain has rapidly evolved in the digital era, incorporating digital and electronic technologies throughout its entire end-to-end process [46]. Eyadema [47] investigated cyber threats to the supply chain, encompassing digital transformation, computer electronics, software updates, and network firmware applications. Cyber supply chain attacks were identified across the software development life cycle, the end-to-end electronic chip manufacturing life cycle, and supply chain management software. The results highlighted challenges within the supply chain, such as intricate IT/OT operations, the update paradox, delays in legacy system updates, the absence of integrated security solutions, and inadequate hardware/software network monitoring tools. Marcu and Hommel [48] explored the intricacies of fault management in the context of IT services outsourced to external providers. They emphasised the challenges arising from the division of services among multiple providers, each responsible for distinct aspects of service implementation, operation, and maintenance. The research highlights the critical need for effective inter-organisational fault management to address the complexities and autonomy inherent in multi-domain environments typical of outsourced IT services. The study underscores the importance of a robust fault management system at the system layer, essential for maintaining service quality and reliability in distributed service delivery settings. This study offers valuable insights for organisations relying on outsourced IT services.

3.4. Cyber Security Culture Framework and IT Governance

Asset valuation can reflect a range of differing issues, including 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 cyber security culture framework (CSCF), as set out by Georgiadou et al. [16] (p. 3), which combines both "external" human factors and "internal" individual notions, at two levels: the organisational level and the individual level. The organisational level encompasses factors related to an organisation'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 behaviours. Each level is further divided into different dimensions. The framework thus distinguishes between the organisational and individual levels, each consisting of multiple dimensions that collectively contribute to a comprehensive understanding and evaluation of an organisation'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 [49] is the latest version of the framework and was 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 organisations to ensure effective control and governance over their IT processes and mitigate IT-related risks. The need to adhere to these practices has led to the development of various software applications under the umbrella term "Governance, Risk and Compliance" (GRC). This is portrayed as a structured way to align IT with business goals while managing risks and meeting all industry and government regulations. It includes tools and processes to unify an organisation's governance and risk management with its technological innovation and adoption. It is emerging as a new software system produced by niche players such as OneTrust [50] and Archer [51], or as a module within ERP systems like SAP [52] and Oracle [53].

A risk assessment of IT assets will normally entail the identification of vulnerabilities, threats, and asset values. As noted above in Section 2, UML can provide a useful communications medium for stakeholders to discuss and collaborate effectively during risk assessment. The CORAS model-based method, noted above [30], was one of the first methods for conducting security analyses that adopted a graphical or model-based approach [54].

3.5. Regulations, Legislation, and International Standards

In the USA, the new regulatory and compliance objectives issued by the Cybersecurity and Infrastructure Security Agency in 2022 [55] 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 [56] 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).

In Europe, EU member states have recently revised the 2016 Network and Information Systems (NIS) Directive in response to several widely publicised and damaging cyberattacks. The NIS2 Directive [57] strengthens security requirements, and member states have until October 2024 to comply; it obliges companies to routinely evaluate cybersecurity risks, set up protocols for managing incidents, apply necessary technical and organisational safeguards, establish continuity strategies for business operations, and fortify the security

of their supply chains. These directives are designed to proactively handle cybersecurity threats, efficiently manage cyber incidents, lower the chances of cyberattacks and information breaches, and guarantee the resilience of operations and the security of the supply chain. To "identify, assess and address your risks" is a recommended first step in achieving compliance [58] (p. 8). Further, the Digital Operational Resilience Act (DORA) [59] is a European Union regulation that came into effect on 16 January 2023 and is set to be fully implemented by 17 January 2025. Its primary objective is to strengthen cybersecurity measures in financial institutions, including banks and insurance companies. DORA requires these entities to institute a comprehensive ICT risk management framework to safeguard against various threats, such as unauthorised access. The management of these institutions is responsible for actively overseeing and updating this framework. The overarching aim is to guarantee robust digital resilience and reduce ICT-related risks within the financial sector. However, the DORA regulations do not offer any solution to the subjectivity issue related with the risk.

Of the international standards relating to risk management, international standard ISO 27001 [60] requires organisations to demonstrate their ability to manage various aspects of information security risk to attain the ISO certification. This involves providing evidence of managing information security risks, implementing actions to mitigate these risks, and applying suitable controls. Risk assessments are essential for compliance with ISO 27001 standards. While ISO 27001 does not provide a specific risk assessment methodology, ISO 27005 [61] offers detailed guidance on information security risk management, including the importance of accurately assessing and evaluating assets. ISO 27005 also guides organisations in identifying, assessing, evaluating, and addressing security vulnerabilities. While it does not specify a method to calculate an asset's value, ISO 27005 underscores the importance of correctly understanding and evaluating assets in risk management. It also acknowledges that risk assessments can be subjective, with uncertainties stemming from the evaluator's judgments.

ISO 27001 is also aligned with another international standard, ISO 31000 [62], which provides guidelines on how to organise risk management in organisations. ISO 31000 defines risk as the impact of uncertainty on objectives. This definition highlights that risk involves the potential for unpredictable events or conditions that affect the achievement of specific goals. It is not focused solely on information security risks, but rather can be applied to a wider range of business risk scenarios. Kosutic [63] has examined the relationship between the two standards and suggested a model demonstrating the overlap of some of the main areas of risk in organisations (Figure 2). Here, we are concerned with information security risk, which encompasses all of cybersecurity and a part of information technology.

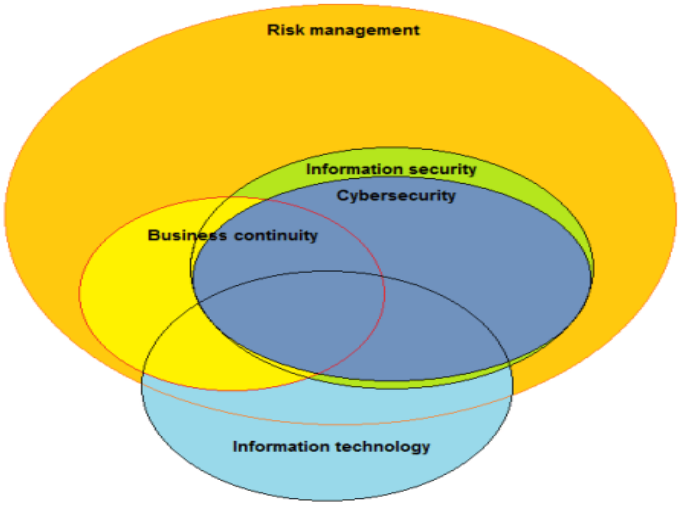

Figure 2. Information security risk and related risk areas. Source: Kosutic [63].

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

RQ1. How can subjectivity in assessing IT asset values be addressed?

RQ2. Can the cyber security culture framework be used to design a flexible risk management system for valuing IT assets in organisations?

4. Conceptual Model: An Extended Cyber Security Culture Framework

The conceptual model for this study (Figure 3) combines elements of the CSCF [16] with asset valuation, supply chain risk, and enhanced objectivity concepts and comprises dimensions at two levels: organisational and individual. At the organisational level, these dimensions are:

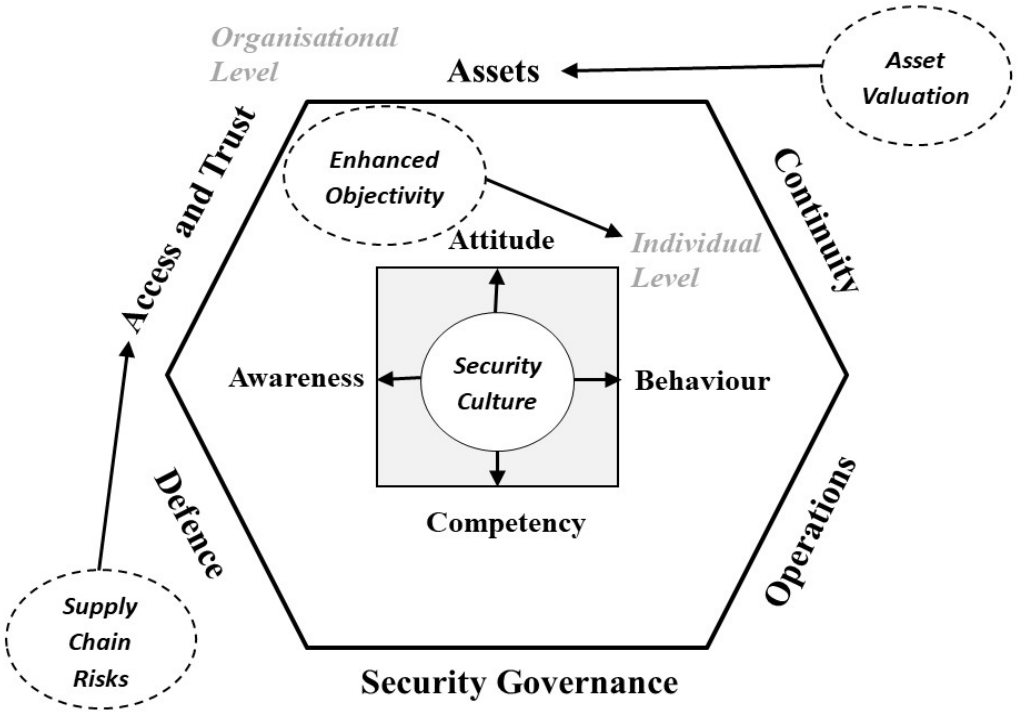

Figure 3. The conceptual model for the research study.

Assets: People, buildings, machines, systems, and information assets. This dimension also includes policies that enforce different levels of confidentiality, availability, and integrity controls. Asset valuation by mitigating subjectivity is the approach adopted here.

Continuity: Aims to ensure the continuity of operations, services, and production for the organisation 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 organisation, clarifying different roles and permissions. It also addresses interactions with third-party entities such as suppliers, customers, and authorities. Supply chain cybersecurity issues are also taken into account here. Mitigating third-party security risks involves contractual agreements and access control measures, but managing supply chain risks encompasses securing products and services throughout their lifecycle, and involves challenges such as vetting suppliers' cybersecurity practices, monitoring threats, and planning for continuity in disruptions.

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

Defence: Emphasises 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 organisation.

The individual level dimensions, which are central to enhancing objectivity in asset valuation, 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 organisation's security policies and procedures.

The conceptual model also embodies principles of the COBIT 2019 framework for IT governance. The assets dimension is further classified under four categories; applications, 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 [49]. "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 the acquisition and implementation of IT resources.

In summary, a conceptual model was developed to act as a basis for system design. To engender an objective assessment of IT asset values, the segregation of duties approach was incorporated into the system design, allowing for 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.

5. Results: System Design and Operation

5.1. System Design

The proposed asset-based risk analysis system builds upon the conceptual model and employs segregation of duties principles to increase the accuracy of human-factor asset value assignment and is aligned with the ISO 27001 standard. As regards risk assessment, ISO 27001 recommends organisations consider vulnerabilities and threats, evaluate the potential impacts of these threats, and then implement appropriate security controls. In this context, a specific risk calculation method is not mandatory, but organisations are required to consistently and effectively apply their risk management processes in a manner that meets their specific needs. A flexible risk assessment system, incorporating asset valuation and supply chain risk concepts, is portrayed in Figure 4, illustrating the class diagram for accommodating the six organisational level dimensions of the CSCF (Assets, Continuity, Access and Trust, Operations, Defence, and Security Governance). Companies can still continue to use their own risk calculation approach as a function of vulnerabilities and threats. In this study, the focus was on the most important parameter of the risk calculation: asset value.

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 categorisation taken from the COBIT 2019 Asset Management process [64]. "Importance level" considers the Continuity and Operations CSCF dimensions. (Asset ID will be numerical and will be auto-generated rather than user-given). "Importance level" is a number that ranges from zero to ten needed for impact analysis, with zero indicating no impact and ten 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.

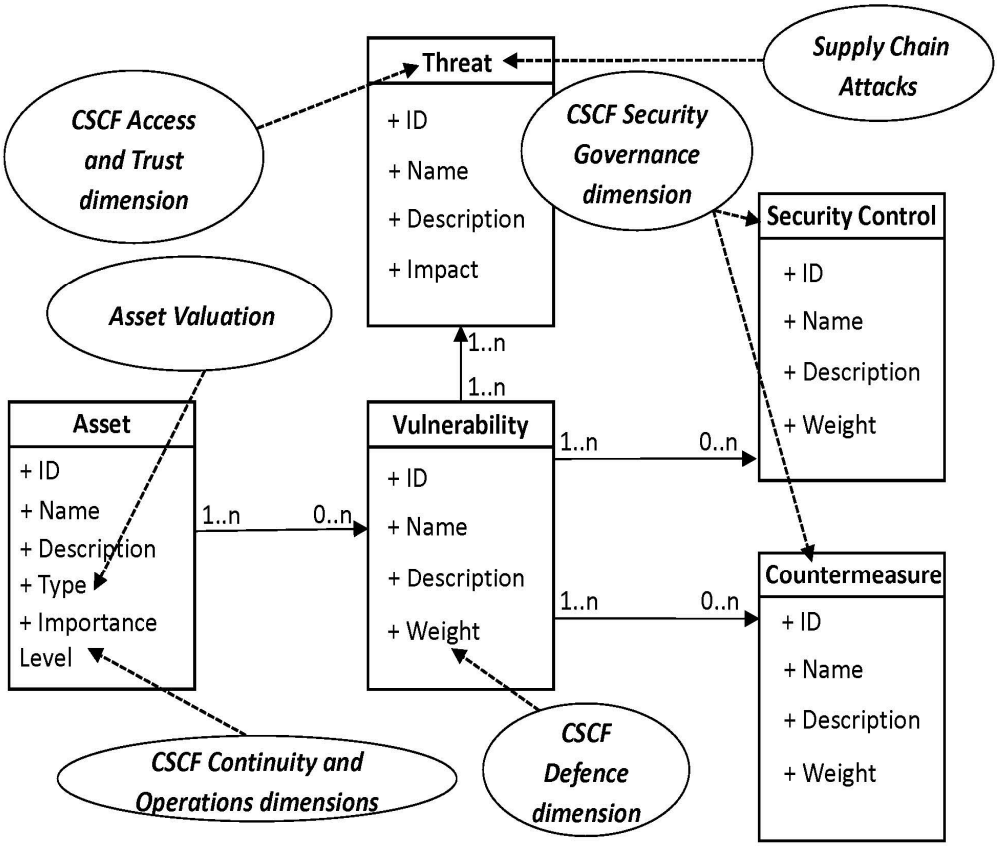

Figure 4. Flexible risk assessment system object classes and relationship to CSCF dimensions.

The Vulnerability object is related to all four other object classes in the system (the 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 is related to at least one vulnerability. This contains the ID, name, description, and weight attributes. The weight attribute is related to the CSCF Defence 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 ranging from zero to ten that is used to help calculate the severity of the exploitation of this vulnerability to the asset, with zero meaning no impact and ten meaning serious damages to the asset.

The Threat object class considers the CSCF 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 that could be threat sources. The Threat object class, similar to the previous classes discussed, has the ID, name, description, and impact attributes. Threat objects are associated with Vulnerability objects.

The Countermeasure and Security Control object classes consider the CSCF Security Governance dimension. The Countermeasure object has the 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 the ID, name, description, and weight attributes. These security controls are supplied by the organisation and will reflect the organisation's preferences, as included in the ISO 27001 information security management system standard. Some organisations might want to have certain

controls involved that will seek to minimise 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 5). 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:

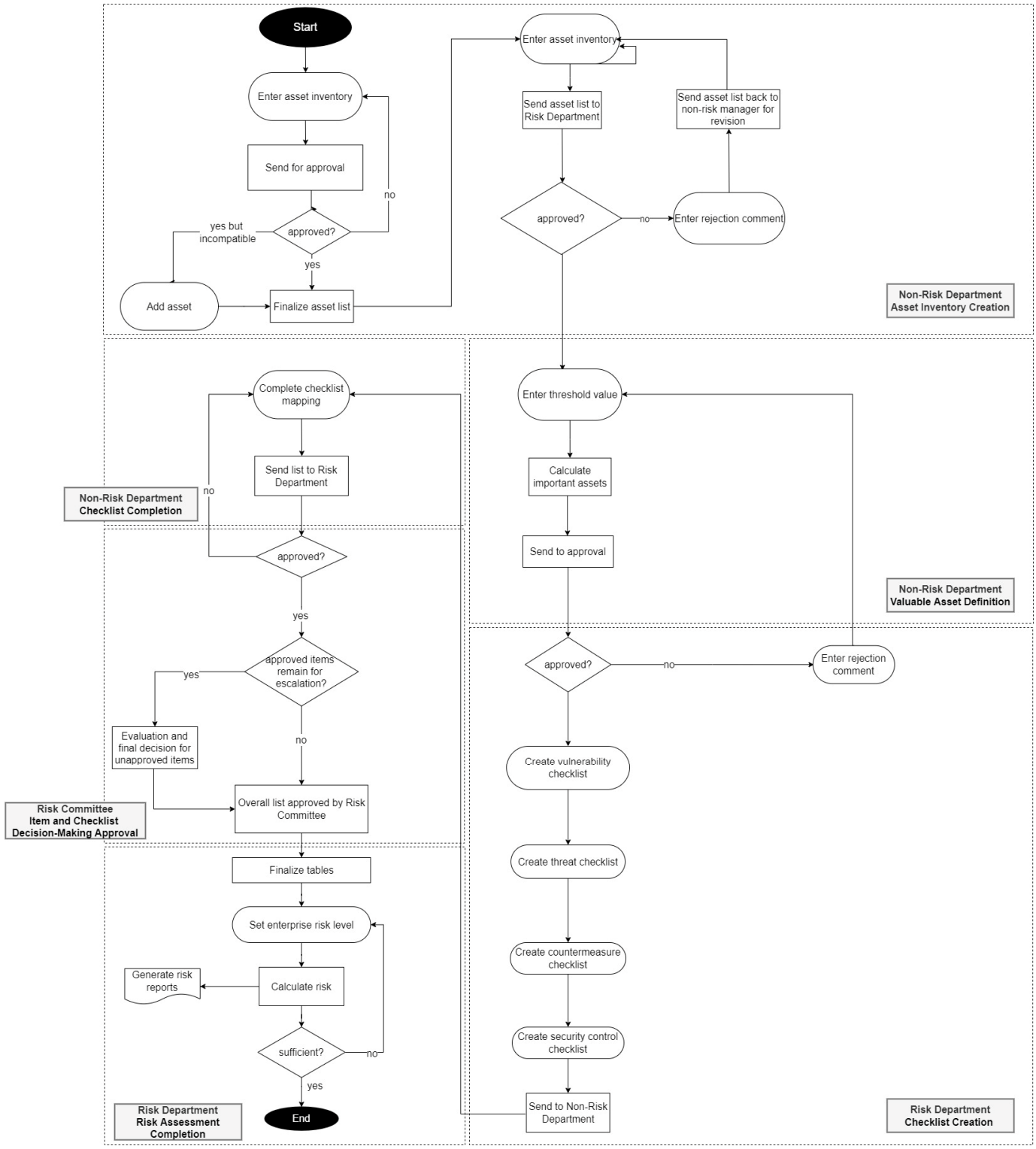

Figure 5. Activity diagram representing system operation.

Non-risk department employee: These 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 organisation 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: These are individuals who work directly in the organisation'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 organisation.

The input from different users fulfilling different roles within the organisation helps improve the accuracy of 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 organisation, 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 2), the incorporation of the CSCF dimensions (Operations, Continuity, Governance) into the system design and operation (as shown in Figure 4) means that wider risks are considered in the context of their impact on the IT assets of the organisation.

5.2. 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. First, information assets are categorised, such as people, buildings, machines, systems, applications, information, infrastructure. Then, questionnaire responses are used to determine their criticality (an exemplar questionnaire is included in Appendix A; the non-risk department manager decides which questions are most appropriate). The non-risk department manager then checks the lists of assets and may approve all or approve some and update or erase some of the assets. After the asset list is completed, the non-risk department manager enters the values that apply 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 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. This can be accomplished by using a survey or questionnaire to gather information from, and about, asset owners. An example of such a questionnaire is included in Appendix A. Part I of the questionnaire is aimed at determining asset values, whilst Part II gathers data relating to the asset owners, utilising individual-level questions to assess the qualifications and security awareness of asset owners in non-risk departments. To ensure objectivity in this prioritisation 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 categorisation, 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 that 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 so that they can 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 items 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 utilised to determine asset values. Moreover, individual factors such as Attitude, Awareness, Behaviour, and Competency from the CSCF 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 that 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 acquire a top-line view of the company's IT risk position and a 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 reset the risk level to a higher or lower level, and the system will automatically recalculate the risks.

In this calculation, the asset priority level is utilised, 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.

6. Validation and Discussion

6.1. Validation Survey

The system outlined above is an example of how the principles embodied in the conceptual model 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 2 above, 16 practitioners were contacted to gain some feedback on the value of the proposed design. The eight 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 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 believed 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 6–8).

Table 2. Survey responses regarding the 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 minimise 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 company sizes, 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 2–4).

6.2. Conceptual Model Review

The conceptual model, upon which the system design is based, integrates the CSCF, asset valuation, supply chain risks, and enhanced objectivity approaches, facilitating a more holistic view of the IT risk assessment process as an extended CSCF. This is accomplished by conducting a thorough assessment of IT assets, while trying to ensure that the evaluation remains unaffected by potential inaccuracies or misjudgements stemming from individual viewpoints that may not be entirely correct or accurate. Furthermore, it allows a detailed, objective assessment of asset values in line with COBIT 2019 through UML modelling, with 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 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.

6.3. Balancing Objectivity and Subjectivity

This research highlights a philosophical dilemma in IT risk assessment related to the subject–object relationship, as emphasised by philosophers such as Heidegger and others [65]. This dilemma is evident in risk assessments owing to the relationship between the asset and its owner. An objective risk assessment should be devoid of personal opinions based on biased and incomplete information, thus eliminating subjectivity. Conversely, human factors play a pivotal role in cybersecurity, and the contributions of individuals must be acknowledged. This seems to present a contradiction: conducting an assessment independent of personal opinions while considering the contributions of asset and risk owners from a human factors' perspective. The conceptual model put forward here tackles this dilemma by systematically incorporating human factors through surveys whilst minimising the margin of error from subjectivity by adhering to the principle of separation of duties.

Notably, standards such as ISO 27001, 27005, and 31000 recognise the issue of subjectivity but do not offer a concrete solution. These standards also recommend identifying the risk owner and considering the specific threats they face. Typically, the risk owner is also the asset owner, suggesting that information assets are intrinsically linked to the individuals managing them. Risk assessment should attempt to both minimise subjectivity and yet also integrate human factors. The approach put forward in this article aims to achieve this by applying the principle of separation of duties and gathering viewpoints from various employees to find the appropriate balance between objectivity and subjectivity for a better risk assessment.

7. Conclusions

In a technology-driven world with numerous cyber threats, effective IT risk management is vital. This paper introduces a model to enhance security culture and minimise personal bias in IT risk assessments. It proposes a "segregation of duties" strategy for more accurate asset valuation for risk evaluation, particularly effective in larger organisations with dedicated risk management teams. The model's effectiveness is validated by feedback from professionals across various sectors. The conceptual model and system design discussed in this article respond to the two research questions set out in Section 2: How can subjectivity in assessing IT asset values be addressed (RQ1)? Can the cyber security culture framework be used to design a flexible risk management system for valuing IT assets in organisations (RQ2)? The system, which employs UML in the design to clarify the procedure, 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 also highlights the value of using UML in an information security domain, the flexibility of UML allowing for customisation of the risk management system according to the size and specific needs of organizations. The system is based on a flow of tasks that makes 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. In addition, the exemplar questionnaire (detailed in Appendix A) is based on the principles of CSCF for asset valuation. Data gleaned from such a questionnaire can provide insights into the security awareness levels of asset owners, enabling the enhancement of the company's security posture through targeted training for these individuals.

The research presented here has its limitations. The method of risk assessment and related aspects makes certain assumptions that will not always apply in all organisations.

Indeed, the survey 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-sized 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. Indeed, the rationale and justification for the developed model and system design can be seen in the context of an attempt to address the issues of subjectivity in risk assessment noted in Section 6.3 above. The evident paradox of subjectivity vs. objectivity is one that challenges risk assessment in most business environments and has brought a range of responses, including new maturity models for risk assessment in project management [3] and, in quality management systems, new design elements that "can be incorporated into quality risk management tools that may help counteract the adverse effects of human heuristics" [66] (p. 76). The conceptual model and system design presented here are not seen as a definitive solution to this problem, but rather as a new way in which the challenge can be met in the context of IT security and asset valuation.

To some, in this age of digital transformation, with the metaverse and quantum computing on the IT horizon [67], the system outlined here may appear simplistic and outdated in its approach. It is maintained here that this is not the case. Rather, it reflects the dearth of proven approaches for mitigating subjectivity in IT asset valuation and risk assessment, as evidenced in the growing focus on this issue in the recent literature. As Nost et al. [32] (para. 8) note "to remediate vulnerabilities and security gaps and acquire 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 entails a hybrid model that can be built upon and developed by other researchers and practitioners and is amenable to the incorporation of digital technology access and support (mobile, analytics, cloud).

There are also wider dimensions to this problem that warrant further research. The implications of integrated supply chains, where companies have access to each other's systems and technologies [68], 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 [69] (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—which include the consideration of additional human factors and business aspects—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.

Institutional Review Board Statement: Not Applicable. No humans or animals were studied, and thus the university Ethics Committee did not need to be consulted.

Informed Consent Statement: Survey respondents agreed to the use of their anonymized responses for research purposes.

Data Availability Statement: The original contributions presented in the study are included in the article. Data provided by the survey respondents was done on the basis of anonymity and thus further detail is unavailable in the public domain. Further inquiries can be directed to the corresponding author.

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 conflicts of interest.

Appendix A. Exemplar Questionnaire for Asset Valuation

The questionnaire should be filled out by the staff in the non-risk department most closety related to the asset (the asset owners), and then this information should be reviewed by the manager of the non-risk department. It is subsequently shared with the risk department specialist. This process is depicted in the activity diagram, representing system operation, in Figure 4. In the survey, only one response should be marked for each question. If assets are grouped together, the questions should be answered considering the most critical and important asset in the group. The rationale for each selected response should be written in detail so that when it is presented to the risk department specialist or the risk committee, a more in-depth consideration can be conducted.

The survey questions should be answered assuming that Ideal conditions prevail as regards the business processes within which information assets are found and operate. This approach allows the calculation of asset values, assuming ideal process conditions. A comparison of actual vs. ideal process conditions can support a gap analysis that provides information about the asset's risk status. Although the primary purpose of the survey is to determine the asset's value, it can thus also be useful for risk assessment.

The survey consists of two sections. Part I (Appendix A.1) determines the asset values (Questions 1–17). Part II gathers data relating to the asset owners (Questions 18–21). Part II (Appendix A.2) utilises individual-level questions to assess the qualifications and security awareness of asset owners in non-risk departments. For instance, only when the awareness level of the non-risk department employee surpasses a certain threshold should the risk expert evaluate asset values by relying on his/her opinion. If this threshold is not met, the risk department specialist will advise the non-risk department manager to re-execute the analysis. This process helps to ensure the quality and reliability of the risk assessment. Answer choices a, b, c, d, and e, correspond to scores 1, 2, 4, 8, and 16, respectively, for each question. After answering all questions, the scores are added up. In Part I, the asset value is assessed as low, moderate, high, or critical (Table A1); in Part II, the asset owner's value is rated as good/could be improved/should be improved/ must be improved (Table A2).

Table A1. Part I Asset Valuation (Questions 1–17).

Survey Score	Asset Value
25–50	Critical
50–75	High
75–125	Medium
>125	Low

Table A2. Part II Asset Owner's Valuation (Questions 18–21).

Survey Score	Asset Owner's Value
8–16	Good
16–24	Could be improved
24–40	Should be improved
>40	Must be improved

Appendix A.1. PART I: Asset Valuation: Organizational-Level Dimension in CSCF

1. **Confidentiality: Potential damages that may occur if the most critical information processed by your asset group is disclosed or captured by unauthorised individuals:**
   a) No damage occurs, the organization and related individuals continue their activities;
   b) Damages that may negatively affect the users of the asset occur.
   c) Damages that may negatively affect the department of the asset occur.
   d) Damages that may negatively affect the entire organization occur.
   e) Damages that may negatively affect the entire organization and its stakeholders occur.
2. **Integrity: Potential damages that may occur if the content of the most critical information processed by your asset group is altered by unauthorised individuals:**
   a) No damage occurs, the organization and related individuals continue their activities.
   b) Damages that may negatively affect the users of the asset occur.
   c) Damages that may negatively affect the department of the asset occur.
   d) Damages that may negatively affect the entire organization occur.
   e) Damages that may negatively affect the entire organization and its stakeholders occur.
3. **Availability: What is the maximum duration of service downtime you can tolerate during peak usage periods for the services dependent on the assets in your group?**
   a) More than 48 h.
   b) Between 24 and 48 h.
   c) Between 8 and 24 h.
   d) Between 4 and 8 h.
   e) Less than 1 h.
4. **Answer questions for information asset categories such as people, buildings, machines, systems, applications, information, and infrastructure.**
   A. **Are there rules or guidelines (e.g., security policies, compliance requirements, operational guidelines) that help protect and manage the assets of our organization?**
      a) Yes, comprehensive rules/guidelines.
      b) Yes, but they need improvement.
      c) Neutral.
      d) No, insufficient rules/guidelines.
      e) No rules/guidelines at all.
   B. **How would you rate the economic value of the assets (for which you are responsible) to our organization's operations (such as software, information, facilities)?**
      a) Extremely valuable (purchase decision given by management board).
      b) Very valuable (purchase decision given by CIO).
      c) Moderately valuable (purchase decision given by department manager and IT manager).
      d) Slightly valuable (purchase decision given by department manager).
      e) Not valuable (purchase decision given by asset owner).
   C. **How difficult is it to replace a specific IT asset in the event of malfunctions, security breaches, or other IT-related incidents? Please select the option that best describes your organization's approach.**
      a) International Procurement (greatest difficulty): Requires sourcing the replacement from international vendors, involving extended delivery times and potentially complex logistics.

b) National Procurement: Involves obtaining the asset from vendors within the country but outside the local region, which can be time-consuming due to distance and shipping.
c) Regional Sourcing: The asset is sourced from suppliers outside the city or local area, necessitating additional time for procurement due to regional distance.
d) City-Wide Sourcing: Replacement can be found within the nearest big city but may require sourcing from specific vendors, offering a moderate level of difficulty and time commitment.
e) Quick, Local Procurement (lowest difficulty): The asset can be easily and quickly replaced from local stores or supermarkets, ensuring immediate availability and minimal downtime.

5. **Business continuity: how confident are you in the resilience of our critical assets to ensure smooth business operations in the event of unexpected disruptions?**
   a) Very confident in the resilience and backup strategies of our critical assets.
   b) Somewhat confident; some assets are well-protected, but others need more robust plans.
   c) Neutral; unsure about the resilience levels of our assets.
   d) Somewhat unconfident; many assets lack sufficient protection or backup plans.
   e) Not confident at all; our critical assets are vulnerable to disruptions.
6. **Crisis management: What measures are in place to protect our key assets, thereby safeguarding our reputation and maintaining the interests of our partners during unexpected events?**
   a) Comprehensive crisis management plan.
   b) Regular communication with partners.
   c) Limited or no specific steps.
   d) Not sure.
   e) Nobody in the company knows.
7. **Access: How well do you think we control who can access our resources and information?**
   a) Very well (zero trust access management).
   b) Adequately (identity access management solution is used).
   c) Neutral (VLAN segmentation and we have a firewall).
   d) Inadequately (no network segmentation but we have a firewall).
   e) Poorly (we do not have a firewall).
8. **Trust: How do we make sure that our interactions with outside parties like suppliers and customers are secure and trustworthy?**
   a) SLA and regular audits and reviews.
   b) SLA.
   c) Basic security measures.
   d) Verbal confirmation.
   e) It does not exist.
9. **Data security: How confident are you in the security of the data and systems in your area of responsibility, which are shared with our third-party vendors?**
   a) Highly confident.
   b) Moderately confident.
   c) Neutral.
   d) Somewhat unconfident.
   e) Not confident at all

10. **Operations: Do our daily operational practices incorporate measures to protect and secure our key assets?**
    a) Always; asset security is a top priority in all our operations.
    b) Often; we regularly consider asset security in our operational decisions.
    c) Sometimes; asset security is considered, but not consistently.
    d) Rarely; asset security is seldom a focus in our daily operations.
    e) Never; we do not integrate asset security into our operational practices.
11. **Asset security: Are there any areas in our daily operations where you think security of our assets could be improved?**
    a) Yes, many areas.
    b) Yes, a few areas.
    c) Neutral.
    d) Not many areas.
    e) No, not at all.
12. **Technology protection:** Do you believe that our current technology infrastructure enhances the security of our assets?
    a) Strongly agree; our technology significantly enhances asset security.
    b) Agree; our technology generally supports asset security.
    c) Neutral; unsure about the impact of our technology on asset security.
    d) Disagree; our technology does little to improve asset security.
    e) Strongly disagree; our technology infrastructure weakens asset security.
13. **Security procedures: Are you aware of the procedures to follow in the event of a security breach or incident involving our assets in your responsibility?**
    a) Fully aware and trained.
    b) Somewhat aware.
    c) Neutral.
    d) Not very aware.
    e) Unaware.
14. **Governance: How well do you think we plan and manage our efforts to keep our information assets safe?**
    a) Very effectively.
    b) Effectively.
    c) Neutral.
    d) Ineffectively.
    e) Very ineffectively.
15. **Evaluation: Do we have effective methods to evaluate the success of our asset security management?**
    a) Yes, very comprehensive and effective evaluation methods.
    b) Yes, but our evaluation methods could be improved.
    c) Neutral; not sure about the effectiveness of our evaluation methods.
    d) No, our methods for evaluating asset security are not very effective.
    e) No, we lack any methods to evaluate asset security effectiveness.
16. **Leadership: How visible and involved are our senior leaders in promoting cybersecurity practices for asset security?**
    a) Highly visible and involved.
    b) Moderately visible and involved.
    c) Neutral.
    d) Seldom visible and involved.
    e) Not visible or involved at all.

17. Empowerment: Do you feel encouraged to provide feedback or suggestions on our cybersecurity policies and practices?

a) Strongly encouraged.
b) Encouraged.
c) Neutral.
d) Discouraged.
e) Strongly discouraged.

Appendix A.2. PART II: Asset Owner's Valuation: Individual-Level Dimension in CSCF

18. Attitude

A. Do feel informed and involved in our organization's cybersecurity policies and initiatives?

a) Very informed and involved.
b) Somewhat informed and involved.
c) Neutral.
d) Not informed or involved.
e) Completely unaware and not involved at all.

B. Do you think the training and resources provided by our organization make you feel prepared to handle cybersecurity challenges?

a) Highly prepared.
b) Reasonably prepared.
c) Neutral.
d) Unprepared.
e) Completely unprepared.

C. How responsible do you feel personally for maintaining cybersecurity in your daily tasks?

a) Strongly feel responsible.
b) Feel responsible.
c) Neutral.
d) Do not feel very responsible.
e) Do not feel responsible at all.

19. Awareness

A. How well do you think you know and understand the organization's information security policies and procedures?

a) Very well.
b) Moderately well.
c) Neutral.
d) Not very well.
e) Not at all.

B. Are you aware of your specific roles and responsibilities in ensuring information security within the organization?

a) Highly aware.
b) Aware.
c) Neutral.
d) Not really aware.
e) Totally unaware.

20. Behaviour

A. How often do you see people following our security rules and guidelines in their daily work? (Are you aware of, and actively report, any security policy violations or suspicious activities? Have you noticed any instances where security rules were not followed?)

a) Always.
b) Often.
c) Sometimes.
d) Rarely.
e) Not sure.

B. Do you consistently adhere to the organization's information security policies and procedures in your daily work?

a) Always.
b) Often.
c) Sometimes.
d) Rarely.
e) Not sure.

21. Competency

A. How confident are you in your ability to follow our security rules and guidelines? (Do you feel equipped with the necessary skills and knowledge to comply with our organization's cybersecurity policies?)

a) Very confident.
b) Confident.
c) Neutral.
d) Not very confident.
e) Not confident at all.

B. Do you think your company provides enough training to help you understand and follow our security practices?

a) Training is very good.
b) Training is reasonable.
c) Neutral.
d) Training is not really good enough.
e) Training is poor and not fit for purpose.

References

1. Zwikael, O.; Ahn, M. The effectiveness of risk management: An analysis of project risk planning across industries and countries. *Risk Anal.* **2011**, *31*, 25–37. [CrossRef]
2. Zayed, T.; Amer, M.; Pan, J. Assessing risk and uncertainty inherent in Chinese highway projects using AHP. *Int. J. Proj. Manag.* **2008**, *26*, 408–419. [CrossRef]
3. 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*; Vajjhala, N.R., Strang, K.D., Eds.; IGI Global: Hershey, PA, USA, 2022; pp. 29–52. [CrossRef]
4. Carleton, J.; Krishnamoorthi, S. *Digital Risk: The Security Challenge Beyond Your Perimeter*; Frost & Sullivan White Paper; Frost & Sullivan: Santa Clara, CA, USA, 2019.
5. Karlsson, F.; Hedström, K.; Goldkuhl, G. Practice-based discourse analysis of information security policies. *Comput. Secur.* **2017**, *67*, 267–279. [CrossRef]
6. Awati, R. Segregation of Duties (SoD). 2023. Available online: https://www.techtarget.com/whatis/definition/segregation-of-duties-SoD (accessed on 8 August 2023).
7. Irizar, J.; Wynn, M. Centricity in Project Risk Management: New Dimensions for Improved Practice. *Int. J. Adv. Intell. Syst.* **2015**, *8*, 209–218. Available online: https://eprints.glos.ac.uk/2429/ (accessed on 3 January 2024).
8. Vandezande, N. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Comput. Law Secur. Review* **2024**, *52*, 105890. [CrossRef]
9. Habbal, A.; Ali, M.K.; Abuzaraida, M.A. Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Syst. Appl.* **2024**, *240*, 122442.
10. Ahmadi, S. Security and Privacy Challenges in Cloud-Based Data Warehousing: A Comprehensive Review. *IJCST* **2024**, *11*, 17–27.
11. Hanneke, R.; Asada, Y.; Lieberman, L.; Neubauer, L.C.; Fagen, M. *The Scoping Review Method: Mapping the Literature in Structural Change Public Health Interventions*; SAGE Publications Ltd.: Thousand Oaks, CA, USA, 2017. [CrossRef]
12. Miles, M.B.; Huberman, A.M. *Qualitative Data Analysis: An Expanded Source Book*, 2nd ed.; Sage: Newbury Park, CA, USA, 1994.
13. Greca, I.M.; Moreira, A.M. Mental models, conceptual models, and modelling. *Int. J. Sci. Educ.* **2000**, *22*, 1–11. [CrossRef]

14. Wand, Y.; Weber, R. Research Commentary: Information Systems and Conceptual Modeling—A Research Agenda. *Inf. Syst. Res.* **2002**, *13*, 363–371.
15. Levering, B. Concept Analysis as Empirical Method. *Int. J. Qual. Methods* **2002**, *1*, 35–48. [CrossRef]
16. Georgiadou, A.; Mouzakitis, S.; Bounas, K.; Askounis, D. A Cyber-Security Culture Framework for Assessing Organization Readiness. *J. Comput. Inf. Syst.* **2020**, *62*, 452–462. [CrossRef]
17. Mishra, S.K.; Mishra, A.; Mohapatra, D.P. Risk Analysis of a system at design level using UML Diagrams. In Proceedings of the 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Mysore, India, 22–25 August 2013. Available online: https://ieeexplore.ieee.org/document/6637170 (accessed on 9 August 2023).
18. Alamri, Q.; Ali, M.A.; Tahir, N.M. Information Technology Risk Management in Oman. In Proceedings of the 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), Langkawi, Malaysia, 28–29 February 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 308–312.
19. 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, London, UK, 15–16 April 2010; pp. 32–41.
20. Bertaux, D. From the life-history approach to the transformation of sociological practice. In *Biography and Society: The Life History Approach in the Social Sciences*; Bertaux, D., Ed.; Sage: London, UK, 1981; pp. 29–45.
21. Krosnick, J.A. Improving question design to maximize reliability and validity. In *The Palgrave Handbook of Survey Research*; Vannette, D.L., Krosnick, J.A., Eds.; Palgrave Macmillan: New York, NY, USA, 2018; pp. 95–101.
22. Kirvan, P.; Irei, A. *Using the FAIR Model to Quantify Cyber-Risk*; TechTarget: Newton, MA, UAS, 2023. Available online: https://www.techtarget.com/searchsecurity/tip/Using-the-FAIR-model-to-quantify-cyber-risk (accessed on 9 November 2023).
23. Hedström, K.; Kolkowska, E.; Karlsson, F.; Allen, J.P. Value conflicts for information security management. *J. Stra-Tegic Inf. Syst.* **2011**, *20*, 373–384. [CrossRef]
24. Shypovskyi, V. Enhancing the factor analysis of information risk methodology for assessing cyber-resilience in critical infrastructure information systems. *Political Sci. Secur. Stud. J.* **2023**, *4*, 25–33.
25. Crespo-Martinez, P.E. Selecting the Business Information Security Officer with ECU@ Risk and the Critical Role Model. In *In-ternational Conference on Applied Human Factors and Ergonomics*; Springer: Cham, Switzerland, 2019; pp. 368–377.
26. Middleton, J. *Capita Cyber-Attack: 90 Organisations Report Data Breaches*; The Guardian: London, UK, 2023. Available online: https://www.theguardian.com/business/2023/may/30/capita-cyber-attack-data-breaches-ico (accessed on 20 July 2023).
27. Cram, W.A.; Proudfoot, J.G.; D'arcy, J. Organizational information security policies: A review and research framework. *Eur. J. Inf. Syst.* **2017**, *26*, 605–641. [CrossRef]
28. 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 Gener. Comput. Syst.* **2019**, *97*, 587–597. [CrossRef]
29. Dursun, S.M.; Mutluturk, M.; Taskin, N.; Metin, B. An Overview of the IT Risk Management Methodologies for Securing Information Assets. In *Cases on Optimizing the Asset Management Process*; IGI Global: Hershey, PA, USA, 2022; pp. 30–47. [CrossRef]
30. Fredriksen, R.; Kristiansen, M.; Gran, B.A.; Stølen, K.; Opperud, T.A.; Dimitrakos, T. The CORAS framework for a model-based risk management process. In Proceedings of the Computer Safety, Reliability and Security: 21st International Conference Proceedings, SAFECOMP, Catania, Italy, 10–13 September 2002; Springer: Berlin/Heidelberg, Germany, 2002; pp. 94–105.
31. Weil, T. Risk assessment methods for cloud computing platforms. In Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 15–19 July 2019; IEEE: Piscataway, NJ, USA, 2019; Volume 1, pp. 545–547.
32. Nost, E.; Maxim, M.; Bell, K.; Worthington, J.; DiCicco, H. *The State of Vulnerability Risk Management 2023*; Forrester Report; Forrester: Cambridge, MA, USA, 2023. Available online: https://reprints2.forrester.com/#/assets/2/1730/RES179028/report (accessed on 22 August 2023).
33. Irwin, L. *Conducting an Asset-Based Risk Assessment in ISO 27001*; Vigilant Software: Ely, UK, 2022. Available online: https://www.vigilantsoftware.co.uk/blog/conducting-an-asset-based-risk-assessment-in-iso-270012013 (accessed on 24 August 2023).
34. Loloei, I.; Shahriari, H.R.; Sadeghi, A. A model for asset valuation in security risk analysis regarding assets' dependencies. In Proceedings of the 20th Iranian Conference on Electrical Engineering (ICEE2012), Tehran, Iran, 15–17 May 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 763–768.
35. Tatar, Ü.; Karabacak, B. A hierarchical asset valuation method for information security risk analysis. In Proceedings of the IEEE International Conference on Information Society (i-Society 2012), London, UK, 25–28 June 2012; pp. 286–291.
36. Kassa, S.G.; Cisa, C. IT asset valuation, risk assessment, and control implementation model. *ISACA J.* **2017**, *3*, 1–9.
37. Ruan, K. *Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics*; Academic Press: Cambridge, MA, USA, 2019.
38. Ekstedt, M.; Afzal, Z.; Mukherjee, P.; Hacks, S.; Lagerström, R. Yet another cybersecurity risk assessment framework. *Int. J. Inf. Secur.* **2023**, *22*, 1713–1729. [CrossRef]
39. Berry, H.S. The Importance of Cybersecurity in Supply Chain. In Proceedings of the 11th IEEE International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, TN, USA, 11–12 May 2023; pp. 1–5.
40. Edwards, B.; Jacobs, J.; Forrest, S. Risky Business: Assessing Security with External Measurements. *arXiv* **2019**, arXiv:1904.11052.

41. Youssef, A.E. A Framework for Cloud Security Risk Management Based on the Business Objectives of Organizations. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 186–194. [CrossRef]
42. Dennig, F.L.; Cakmak, E.; Plate, H.; Keim, D.A. VulnEx: Exploring Open-Source Software Vulnerabilities in Large Development Organizations to Understand Risk Exposure. *arXiv* **2022**, arXiv:2108.06259v3.
43. Goyal, H.P.; Akhil, G.; Ramasubramanian, S. Manage Risks in Complex Engagements by Leveraging Organization-Wide Knowledge Using Machine Learning. *arXiv* **2022**, arXiv:2202.10332.
44. Hu, K.; Levi, R.; Yahalom, R.; Zerhouni, E. Supply Chain Characteristics as Predictors of Cyber Risk: A Machine-Learning Assessment. *arXiv* **2023**, arXiv:2210.15785v5.
45. Khani, S.; Gacek, C.; Popov, P. Security-aware selection of web services for reliable composition. *arXiv* **2015**, arXiv:1510.02391.
46. Hammi, B.; Zeadally, S.; Nebhen, J. Security threats, countermeasures, and challenges of digital supply chains. *ACM Comput. Surv.* **2023**, *55*, 316.
47. Marcu, P.; Hommel, W. Inter-organizational fault management: Functional and organizational core aspects of management architectures. *arXiv* **2011**, arXiv:1101.3891. [CrossRef]
48. Eyadema, S.I. Outsource Supply Chain Challenges and Risk Mitigation. Unpublished Doctoral Dissertation, Utica College, New York, NY, USA, 2021.
49. 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).
50. OneTrust. Avoid Uncertainty—Empower Your Operations with Risk-Based Decision Making. 2023. Available online: https://www.onetrust.com/solutions/grc-and-security-assurance-cloud/ (accessed on 24 November 2023).
51. Archer. Archer GRC Solution. Available online: https://www.archerirm.com/content/grc (accessed on 24 November 2023).
52. SAP. Governance, Risk, Compliance (GRC), and Cybersecurity. 2023. Available online: https://www.sap.com/products/financial-management/grc.html (accessed on 24 November 2023).
53. Oracle. Oracle Enterprise Governance, Risk and Compliance Documentation. 2023. Available online: https://docs.oracle.com/applications/grc866/ (accessed on 24 November 2023).
54. Lund, M.S.; Solhaug, B.; Stølen, K. *Model-Driven Risk Analysis: The CORAS Approach*; Springer: Berlin/Heidelberg, Germany, 2010.
55. Nost, E.; Burn, J. *CISA Releases Directives on Asset Discovery and Vulnerability Enumeration*; Forrester: Cambridge, MA, USA, 2022. Available online: https://www.forrester.com/blogs/cisa-releases-directives-on-asset-discovery-and-vulnerability-enumeration/ (accessed on 4 October 2023).
56. Rapid7. Evaluating Vulnerability Assessment Solutions. Available online: https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-vulnerability-assessment-buyers-guide.pdf (accessed on 9 October 2023).
57. EUR-Lex. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Re-Pealing Directive (EU) 2016/1148 (NIS 2 Directive)*; Official Journal of the European Union: Brussels, Belgium, 2022. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 (accessed on 24 November 2023).
58. CyberArk/PWC. *Getting Ready for the NIS2 Directive*; White Paper; CyberArk UK: London, UK, 2023. Available online: https://www.cyberark.com/resources/white-papers/getting-ready-for-nis2?utm_source=google&utm_medium=paid_search&utm_term=emea_english_nl_ie_be_dk_sw_it_es_fr&utm_content=20230220_gb_wc_nis2_get_ready_pwc_wp&utm_campaign=security_privilege_access&gclid=CjwKCAiA6byqBhAWEiwAnGCA4LSZ1FpvLUjXjEyu1LJvBqpKVY73PryI2HnXd_BYvR23uZX74Z19RxoCY9QQAvD_BwE (accessed on 11 November 2023).
59. EUR-Lex. *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*; Official Journal of the European Union: Brussels, Belgium, 2022. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554 (accessed on 11 November 2023).
60. *ISO 27001*; Information Technology—Security Techniques–Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2013. Available online: http://www.itref.ir/uploads/editor/428900b.pdf (accessed on 23 August 2023).
61. *ISO 27005:2022*; Information Technology—Security Techniques—Information Security Risk Management. International Organization for Standardization: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/80585.html (accessed on 23 August 2023).
62. *ISO 31000*; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/65694.html (accessed on 30 June 2023).
63. 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,%20ISO%2027001%20notes%20that%20information%20security%20management%20in%20ISO,already%20compliant%20with%20ISO%2031000 (accessed on 23 August 2023).
64. Harisaiprasad, K. *COBIT 2019 and COBIT 5 Comparison*; ISACA: Schaumburg, IL, USA, 2020. Available online: https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison (accessed on 12 October 2023).

65. Wambacq, J. Subject-Object in Martin Heidegger, Bruno Latour and Manuel De Landa. 2000. Available online: https://constantvzw.org/verlag/spip.php?article79# (accessed on 25 November 2023).
66. O'Donnell, K. Strategies for Addressing the Problems of Subjectivity and Uncertainty in Quality Risk Management Exercises: Part I-The Role of Human Heuristics. *J. Valid. Technol.* **2020**, *16*, 76–84.
67. Wynn, M.; Jones, P. New technology deployment and corporate responsibilities in the metaverse. *Knowledge* **2023**, *3*, 543–556. [CrossRef]
68. Nightingale, C. Managing Cyber Risk through Integrated Supply Chains. *Computer Weekly*, 21 September 2021. Available online: https://www.computerweekly.com/opinion/Managing-cyber-risk-through-integrated-supply-chains?utm_campaign=20211229_ERU+Transmission+for+12/29/2021+(UserUniverse:+364164)&utm_medium=EM&utm_source=ERU&src=8907352&asrc=EM_ERU_198647440&utm_content=eru-rd2-rcpC (accessed on 9 October 2023).
69. 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).