Cybersecurity Culture

Subjects: Business

Contributor: Bilgin Metin , Sefa Duran , Eda Telli , Meltem Mutlutürk , Martin Wynn

Cybersecurity culture, encompassing organizational and individual levels, shapes an organization's values, behaviors, and practices. Its core objective is to protect information technology (IT) assets, sensitive data, and technology infrastructures against cyber threats and reduce IT risks in today's digital-centric business landscape. 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. Asset valuation with enhanced objectivity should be considered in an established security culture. Therefore, mitigating subjectivity in IT risk assessments diminishes personal biases and presumptions to provide a more transparent and accurate understanding of the real risks involved and enhances cybersecurity culture.

risk assessment | asset value | information security | risk management | objective risk assessment | segregation of duties | security culture framework | cybersecurity culture | cybersecurity culture framework

1. Concepts and Methods: Risk Assesment

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" [1] (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 [2], and other limitations include complexity, limited scope, subjectivity, lack of standardisation, and cost [3]. 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 [4]. This has been highlighted by the data breaches and attacks suffered by many organisations in recent years [5], and information security management is being increasingly viewed as an important tool in ensuring organisational continuity [6][7].

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 [8]. 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 [9]. 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 [10], but Nost et al. [11] (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 [12]. 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.

2. Asset Valuation in Risk Assessment

Although there are numerous studies on risk assessment in the literature, only a few focus on determining asset value. Loloei et al. [13], 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 [14] 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 [15] 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 [16] 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. [17] 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. 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 [18].

In addressing the challenge of assessing security practices in large organisations, particularly when integrating third-party services, Edwards et al. [19] 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 [20]. 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. [21] on open-source software vulnerabilities in large organisations underscores a broader concept in cybersecurity: the significance of identifying third-party security risks. This research 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. [22] 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. [23] 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. [24] 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 [25]. Eyadema [26] 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 [27] 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 research offers valuable insights for organisations relying on outsourced IT services.

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 should be an element of the cyber security culture framework (CSCF), and an extended cyber security framework based on Georgiadou et al. [28] (p. 3) is presented as shown in **Figure 1**. The CSCF 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 [29] is the latest version of the framework and was used in this research. 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 [30] and Archer [31], or as a module within ERP systems like SAP [32] and Oracle [33].

A risk assessment of IT assets will normally entail the identification of vulnerabilities, threats, and asset values. As noted above, UML can provide a useful communications medium for stakeholders to discuss and collaborate effectively during risk assessment. The CORAS model-based method, noted above [9], was one of the first methods for conducting security analyses that adopted a graphical or model-based approach [34].

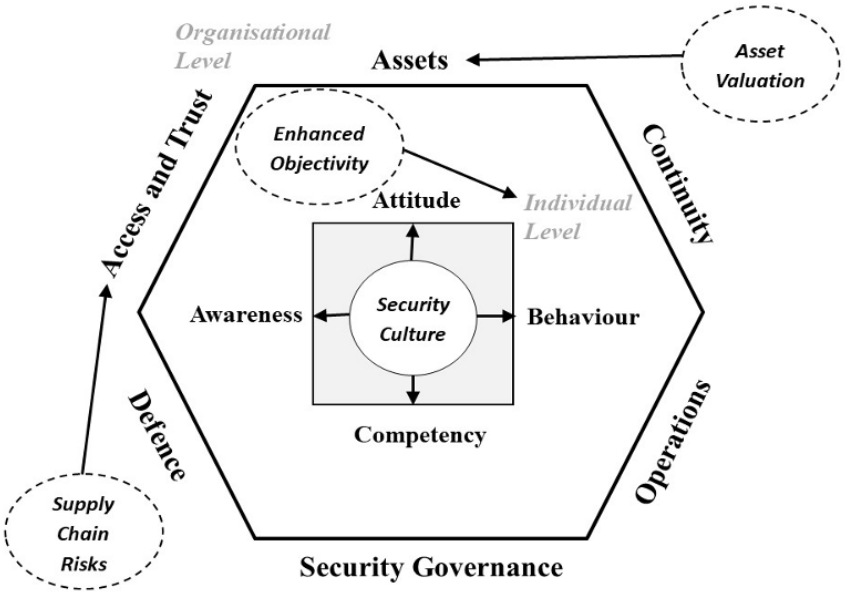

Figure 1. An Extended Cyber Security Culture Framework based on Georgiadou et al. [28]

5. Information Security Regulations, Legislation, and International Standards

In the USA, the new regulatory and compliance objectives issued by the Cybersecurity and Infrastructure Security Agency in 2022 [35] 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 [36] 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 [37] 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 [38] (p. 8). Further, the Digital Operational Resilience Act (DORA) [39] 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 [40] 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 [41] 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 [42], 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 [43] 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, reseaerchers are concerned with information security risk, which encompasses all of cybersecurity and a part of information technology.

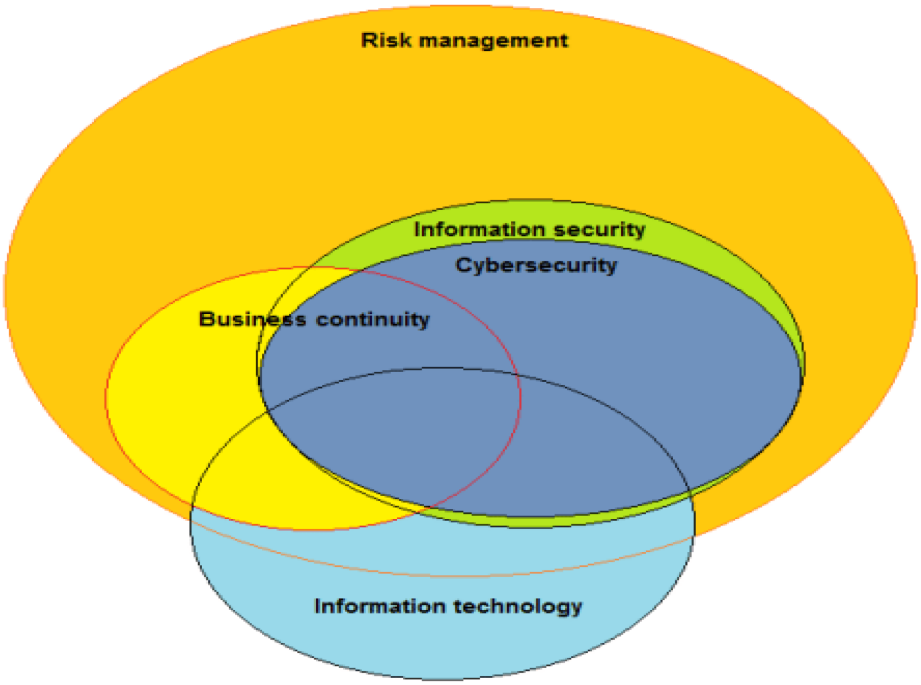

Figure 2. Information security risk and related risk areas. Source: Kosutic [43].

References

1. 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).
2. Hedström, K.; Kolkowska, E.; Karlsson, F.; Allen, J.P. Value conflicts for information security management. J. Stra-Tegic Inf. Syst. 2011, 20, 373–384.
3. 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.
4. 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.
5. 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).
6. 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.
7. 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.
8. 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.

9. 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.
10. 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.
11. 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).
12. 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).
13. 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.
14. 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.
15. Kassa, S.G.; Cisa, C. IT asset valuation, risk assessment, and control implementation model. ISACA J. 2017, 3, 1–9.
16. Ruan, K. Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics; Academic Press: Cambridge, MA, USA, 2019.
17. Ekstedt, M.; Afzal, Z.; Mukherjee, P.; Hacks, S.; Lagerström, R. Yet another cybersecurity risk assessment framework. Int. J. Inf. Secur. 2023, 22, 1713–1729.
18. 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.
19. Edwards, B.; Jacobs, J.; Forrest, S. Risky Business: Assessing Security with External Measurements. arXiv 2019, arXiv:1904.11052.
20. 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.
21. 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.
22. 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.
23. 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.
24. Khani, S.; Gacek, C.; Popov, P. Security-aware selection of web services for reliable composition. arXiv 2015, arXiv:1510.02391.
25. Hammi, B.; Zeadally, S.; Nebhen, J. Security threats, countermeasures, and challenges of digital supply chains. ACM Comput. Surv. 2023, 55, 316.
26. Marcu, P.; Hommel, W. Inter-organizational fault management: Functional and organizational core aspects of management architectures. arXiv 2011, arXiv:1101.3891.
27. Eyadema, S.I. Outsource Supply Chain Challenges and Risk Mitigation. Unpublished Doctoral Dissertation, Utica College, New York, NY, USA, 2021.
28. 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.
29. 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).

30. 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).
31. Archer. Archer GRC Solution. Available online: https://www.archerirm.com/content/grc (accessed on 24 November 2023).
32. SAP. Governance, Risk, Compliance (GRC), and Cybersecurity. 2023. Available online: https://www.sap.com/products/financial-management/grc.html (accessed on 24 November 2023).
33. Oracle. Oracle Enterprise Governance, Risk and Compliance Documentation. 2023. Available online: https://docs.oracle.com/applications/grc866/ (accessed on 24 November 2023).
34. Lund, M.S.; Solhaug, B.; Stølen, K. Model-Driven Risk Analysis: The CORAS Approach; Springer: Berlin/Heidelberg, Germany, 2010.
35. 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).
36. 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).
37. 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).
38. 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_n (accessed on 11 November 2023).
39. 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%3A32022R2554 (accessed on 11 November 2023).
40. 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/42890b.pdf (accessed on 23 August 2023).
41. 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).
42. 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).
43. Kosutic, D. ISO 31000 and ISO 27001—How Are They Related? 2022. Available online: https://advisera.com/27001academy/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/#:~:text=In%20clause%206.1.-,3%2C%20ISO%2027001%20notes%20that%20information%20security%20management%20in% (accessed on 23 August 2023).