International Journal of Information Management Data Insights 5 (2025) 100370

Contents lists available at ScienceDirect

International Journal of Information Management Data Insights

journal homepage: www.elsevier.com/locate/jjimei

Strengthening the UK regulatory framework: Enhancing cybersecurity in supply chains

Betul Gokkaya [a], Konstantina Spanaki [b], Erisa Karafili [a,*]

[a] School of Electronics and Computer Science, University of Southampton, Southampton, United Kingdom
[b] Department of Information Systems and Supply Chain Management, Audencia Business School, Nantes, France

ARTICLE INFO

Keywords:
Supply chain
Security
Risk analysis
NIS framework
Risk

ABSTRACT

The increasing risks associated with cybersecurity in global supply chains present a significant problem, threatening the operational integrity and security of organisations on a global scale. The UK's Network and Information Systems (NIS) Framework, although fundamental in cybersecurity regulation, has significant gaps in effectively addressing the complexities of contemporary global supply chain architectures entangled with quickly advancing cyber threats. In this work, we analyse the UK NIS framework, identify key gaps, and propose solutions drawn from other existing frameworks, e.g., US NIST, EU NIS2. We base this analysis on a comparative evaluation using defined criteria related to supply chain coverage, adaptability, and risk management specificity. We enhanced the cybersecurity in supply chains by proposing novel security requirements plans for each risk profile. Furthermore, we examined various solutions for risk assessments and self-risk assessments for supply chain security. We analysed practical risk assessment approaches, including self-assessment strategies, particularly suited for SMEs. Moreover, we investigated the contracting between supply chains in the context of data and information sharing.

1. Introduction

In today's global business environment, supply chain operations have transformed into intricate networks that involve multiple organisations across different layers. The intricate nature of this system, which enables extensive trade and operational effectiveness, has unintentionally created notable weaknesses, especially in the field of cybersecurity (Zhang & Guin, 2019). As businesses aim to effectively control and simplify their supply chains, the complex relationships between organisations have made it difficult to achieve a complete understanding of supplier networks. The limited visibility, combined with the complex nature of supply chain relationships, greatly hinders organisations' capacity to enforce strong security measures against cyber threats (Alkhadra, Abuzaid, AlShammari, & Mohammad, 2021).

Attackers have redirected their attention to suppliers, particularly those with less rigorous cybersecurity measures, as they are aware of the vulnerabilities that exist inside supply chains. This tactic, referred to as a supply chain attack, exploits compromised suppliers as channels to infiltrate and compromise the final objective with greater efficiency. The consequences of such attacks are not just hypothetical; events like the SolarWinds breach (Alkhadra et al., 2021) have clearly demonstrated the devastating capacity of supply chain cyberattacks, affecting major enterprises, government institutions, and key infrastructures in many industries. The NotPetya attack in 2017 highlighted the significant risks involved in supply chain cyberattacks on critical infrastructures. The origin of this attack can be traced back to a Ukrainian software enterprise that operates in a small family-run firm whose product, M.E.Doc, was used by almost every Ukrainian business for tax filing (Greenberg, 2018). The attackers inserted malicious code into a software update that was then sent to users, including many businesses in Ukraine. The impact of NotPetya was far-reaching, with victims spanning various critical infrastructure entities. These incidents highlight the significance of enhancing the cybersecurity strategy of organisations involved in global supply networks.

In order to facilitate this enhancement, governments, and regulatory agencies have established diverse frameworks and rules with the objective of strengthening cybersecurity in supply chains. Prominent instances encompass the recommendations provided by esteemed institutions such as the National Institute of Standards and Technology (NIST)[1] in the United States, the Network and Information Systems (NIS) (European Union Agency for Cybersecurity (ENISA), 2023) and NIS2 (Commission, 2025) laws in the European Union, and the NIS 2018 guidelines in the United Kingdom (Legislation.gov.uk, 2018).

* Corresponding author.
E-mail addresses: betul.gokkaya@soton.ac.uk (B. Gokkaya), kspanaki@audencia.com (K. Spanaki), e.karafili@soton.ac.uk (E. Karafili).

[1] https://www.nist.gov/

https://doi.org/10.1016/j.jjimei.2025.100370

Available online 2 September 2025

Although these frameworks are a positive advancement in ensuring supply chain security, their shortcomings become apparent when we take into account the ever-changing strategies of attackers and the intricate interdependencies within global supply chains. For example, while the UK NIS 2018 framework offers a foundational approach to securing essential services, it remains high-level and has not been updated to reflect recent developments in cyber threats. In contrast, the updated NIS2 directive in the European Union introduces more stringent requirements, particularly regarding supply chain security, risk management, and incident reporting. The NIST Cybersecurity Framework, on the other hand, provides a voluntary yet detailed and flexible model that emphasises continuous improvement and maturity-based controls. Compared to these more dynamic frameworks, the UK NIS appears less prescriptive and less adapted to modern supply chain complexities, particularly those impacting small and medium-sized enterprises (SMEs). As a result, there is a growing need to critically evaluate the effectiveness of current cybersecurity frameworks within the context of supply chains (Gokkaya, Karafili, Aniello, & Halak, 2024).

Our main goal in this work is to improve supply chain security. In particular, we will identify specific areas that require improvements in a well known cybersecurity regulation framework that is the UK NIS 2018 framework (Legislation.gov.uk, 2018), for simplicity, we will call it the UK NIS framework. Our analysis will identify the gaps in this framework in the context of supply chain security. We decided to focus on this framework (given that it has not been updated yet) in order to provide some useful insights to improve it. We will first perform a comparative analysis of the main cybersecurity frameworks (including the UK NIS one). Building on the analysis findings, we will analyse the limitations of the UK NIS framework in terms of its ability to enhance cybersecurity within supply chains, with a specific focus on various components such as digital service providers, operators of essential services, and information systems utilised in supply chains. Furthermore, we will also provide possible solutions on how to address the identified gaps. Instead of coming up with new solutions that would be difficult to implement in a short period of time by this framework, we opted to identify (when possible) existing solutions or techniques. We believe this will improve the applicability of these solutions to a new, more secure UK NIS framework. Our work will also be useful to other existing and developing frameworks, as they can use our analysis to identify their own gaps and use parts of our proposed solutions to fill these gaps.

Another important step towards improving the cybersecurity of a company and its supply chain in general is to perform a cybersecurity risk assessment. Once the level of risk is established, then actions can be taken to improve the security of the entity and the related supply chain network. Current frameworks do not delve into the details of risk assessment. Furthermore, there is a need to provide an analysis of current risk assessment techniques.

In this paper, we address the above challenge by analysing the current solutions for risk assessment, emphasising self-risk assessment solutions. As the latter can help SMEs, with small or no budget on security, to improve the supply chain risk. Furthermore, we provide five novel risk plans for supply chains, where every plan has an associated level of cybersecurity risk. To develop these novel plans, we took inspiration from existing solutions in the defence space, i.e., UK Def Stan 01-138 (GOV.UK, 2021) and DEFCON (GOV.UK, 2022). For each of our plans, we provide a set of security requirements that are *strongly recommended*, *recommended*, and *desirable* to the supply chain. Supply chain companies can request their suppliers to guarantee these security requirements, depending on the level of risk, and can enforce these requirements using contractual clauses.

Contracting can be a powerful tool to enforce security and privacy requirements in the supply chain. In this paper, to improve the security of the overall supply chain, we will also analyse the supply chain contracting, especially in the case of data and information sharing (Spanaki, Karafili, & Despoudi, 2022).

The paper is organised as follows. In Section 2, we conduct a comparative analysis of major global cybersecurity frameworks, highlighting their limitations in addressing the specific needs of diverse supply chain participants. In Section 3 we identify the gaps in the current UK NIS regulations and provide possible solutions taken from existing frameworks and regulations like the NIST (National Institute of Standards and Technology (NIST), 2018) and NIS/NIS2 (European Union Agency for Cybersecurity (ENISA), 2023). In Section 4, we introduce novel security requirements for each risk profile and cybersecurity risk assessments solutions for supply chain. Supply chain contracting about data and information sharing is discussed in Section 5. We conclude in Section 6 where we summarise the main findings of our paper.

2. Comparative analysis of cybersecurity frameworks for supply chain security

In this section, we explore how major regional cybersecurity guidelines, such as the NIST Framework in North America, the NIS and NIS2 Directives in the EU, the ISO standards, and the UK's NIS Framework, approach the challenge of securing supply chains in the context of evolving cyber threats. For organisations across the supply chain spectrum, particularly those with limited capacity, these frameworks can be complex and resource-intensive, raising questions about their scalability and practical implementation.

To evaluate how well these existing frameworks support effective cybersecurity in diverse supply chain environments, we assess them based on the following criteria:

- Clarity and practical guidance for implementation;
- Cost-effectiveness and scalability across organisations of different sizes;
- Threat-specific risk management relevant to modern supply chains;
- Support for security awareness and training within supply chain actors;
- Vendor and third-party risk management practices;
- Adaptability to emerging technologies;
- Encouragement of collaboration and threat intelligence sharing.

The comparative analysis presented in Table 1 reveals that major cybersecurity frameworks, while offering foundational principles, often lack clear, practical, and scalable guidance for organisations of diverse sizes, capabilities, and resources (Schauer, Polemi, & Mouratidis, 2019). Common gaps across frameworks include a lack of tailored guidance, cost-effective solutions, attention to key threats (e.g., phishing, ransomware), and support for vendor risk management (AL-Dosari & Fetais, 2023). They also lag in adapting to new technologies and fostering collaboration, especially for SMEs. These issues highlight the need for adaptable, context-aware approaches to securing diverse, modern supply chains.

Building on this, our comparative analysis lays the groundwork for evaluating the UK NIS framework, emphasising the need to better address the varied risks and capabilities of supply chain actors, particularly SMEs. The UK NIS is the main cybersecurity regulation for UK supply chains but struggles to offer practical, scalable guidance across diverse organisations. The following section presents a gap analysis to identify areas for improvement and adaptation to modern supply chain challenges.

3. Cybersecurity gaps analysis and solutions in the UK NIS

The NIS Regulations in the UK[2] have been implemented to provide a legal structure that protects the country's crucial national infrastructure

[2] https://www.legislation.gov.uk/uksi/2018/506

Table 1
Challenges in adapting existing guidelines for diverse supply chain needs.

Criteria	Government guidelines and frameworks				
	NIST framework	ISO/IEC standards	ENISA guidelines	NIS/NIS2 directives	UK NIS
Simplified and Tailored Frameworks	Complex and resource-intensive; lacks simplified, modular guidance for SMEs.	Comprehensive but requires certification and extensive resources; not SME-friendly.	Useful resources but lacks prescriptive frameworks tailored to SMEs.	High-level directives that require significant interpretation; not tailored to SME-specific challenges.	High-level and static; lacks detailed, actionable guidance; not tailored to SME-specific needs.
Cost-Effective and Scalable Solutions	High cost of implementation and compliance, unsuitable for limited SME budgets.	Cost of certification and audits is prohibitive for SMEs.	Provides best practices but no scalable implementation models for SMEs.	Implementation and compliance costs are burdensome for SMEs, especially in resource-constrained environments.	Lacks specific cost-effective provisions; generic requirements impose burdens on SMEs without clear scaling.
Focused Threat-Based Risk Assessment	Broad risk categories, does not emphasise SME-specific threats like phishing or ransomware.	Generalised risk assessments fail to focus on common SME-specific threats.	Offers threat landscape reports, but not tailored risk prioritisation for SMEs.	Emphasis on critical infrastructure leaves SMEs' specific risks underrepresented.	Generic risk categories; lacks SME-relevant threat prioritisation and guidance for specific risk profiles.
Employee Awareness and Training	Limited practical advice on SME-appropriate training programs.	Focuses on formal training processes without SME-tailored resources.	Awareness materials exist but are not specific to SMEs' operational contexts.	Mandates training but provides little actionable guidance for SMEs to implement cost-effectively.	Mentions training requirements but lacks practical tools or resources tailored for SMEs.
Vendor and Third-Party Risk Management	Assumes SMEs can enforce compliance on vendors, which is rarely feasible.	Does not address the power imbalance SMEs face with larger vendors.	Provides guidelines but lacks tools for SMEs to monitor vendor risks effectively.	Encourages vendor risk assessment but lacks specific tools or frameworks for SMEs.	Limited guidance on practical vendor risk management; assumes SMEs can enforce requirements in contracts.
Adaptability to Emerging Technologies	Static framework; not easily adaptable to dynamic risks from IoT and cloud technologies.	Lacks flexibility for rapidly evolving technology landscapes.	Limited focus on dynamic adaptation for emerging tech-specific risks.	Reactive rather than proactive in addressing emerging technology risks.	Static, prescriptive; slow to adapt to new technologies and evolving cyber threats.
Collaborative and Community-Based Approaches	Encourages collaboration but lacks mechanisms for structured partnerships for SMEs.	Minimal guidance on fostering collaboration for SMEs.	Promotes collaboration but lacks actionable frameworks for SME-specific needs.	Focused on member state collaboration; limited emphasis on enabling SMEs to participate.	Lacks structured mechanisms for SME collaboration; limited emphasis on shared threat intelligence.

from the growing number of cyber threats. While these regulations are a significant milestone in strengthening the UK's ability to withstand cyber attacks, the constantly evolving nature of cyber threats and rapid technological advancements necessitate regular review and reevaluation of regulatory frameworks.

In this section, we identify and analyse the gaps in the existing UK NIS framework, revealing areas where the framework may be inadequate in tackling modern cybersecurity concerns. In our analysis, we take into account both theoretical knowledge and practical observations, to thoroughly investigate these gaps in many aspects. We organise this section into distinct subsections, each focused on clarifying a particular gap in the NIS framework. Furthermore, we establish the specific areas where the existing framework may require enhancement or adjustment to more effectively safeguard the security of supply chains. We proposed enhancement and/or solutions taken from other frameworks or existing regulations. We will explain each identified gap, provide existing solutions from other frameworks and regulations, and finally propose how these solutions can be incorporated/developed in the UK NIS framework.

Our analysis is useful not only to the improvement of the current UK NIS framework but also for the security aspects of other existing frameworks. The latter can use our analysis to identify their own gaps. Furthermore, the proposed solutions, with a little tweaking, can be integrated into these frameworks as well.

3.1. Operationalisation and measurement of success

The UK NIS framework highlights the significance of developing a national strategy that includes distinct objectives and goals for safeguarding networks and information systems. This framework does not place much importance on the methods of implementation, particular

goals, performance indicators, or metrics for assessing the efficacy of the adapted measures. Hence, creating a big gap between strategies and objectives versus operationalisation and measurement of success.

To address the above gap, we analysed the NIST Cybersecurity Framework (National Institute of Standards and Technology (NIST), 2018) that provides a thorough method for managing cybersecurity risk, effectively addressing the gap in implementation. We conducted a thorough analysis of the NIST Cybersecurity Framework version 1.1, for the sake of simplicity, we will refer to it as the NIST Framework or simply NIST. The NIST Framework does not suffer from the above gap, as it has the following measures in place.

- Measurement of Success: NIST emphasises the use of cybersecurity metrics and measurements to evaluate the efficacy of the security posture. By implementing this method, organisations can create measurements that are in line with the strategic goals.
- Continuous Improvement: NIST recommends an ongoing system of enhancement. This guarantees that the plan stays pertinent in the context of developing cyber risks and technical advancements.
- Customisation to National Context: NIST is highly adaptable and can be tailored to different sectors. It provides a customisable model that can be adjusted to address the specific requirements and vulnerabilities of a nation's vital infrastructure and digital services.

In order to bridge the gap in operationalisation and measurement within the national strategy for the UK NIS, policymakers and regulators in the UK might consider incorporating the concepts and practices of the NIST Framework into their strategic planning and implementation procedures. Possible components of this could include:

1. Developing specific cybersecurity outcomes and activities aligned with the NIS strategic objectives.
2. Establishing clear metrics and indicators for success, based on NIST guidance, to monitor progress and effectiveness.
3. Regularly reviewing and updating the national strategy based on a continuous improvement model, leveraging the iterative approach of the NIST Framework.

3.2. Coordination and consistency

Another major gap in the NIS is ensuring efficient coordination and uniformity among different competent bodies, e.g., the Information Commissioner. Due to the decentralised structure, with many bodies having jurisdiction over various sectors and subsectors, there can be variation in the application of legislation, publication of guidance, and management of cybersecurity issues. Hence, there are variations in the implementation, direction, and overall state of cybersecurity across different sectors. In addition, the use of multiple lists, e.g., those for critical service operators and revocations, and the requirement for collaboration with other agencies, including GCHQ and law enforcement, increases to the difficulty of maintaining a consistent and efficient cybersecurity framework.

To address this lack of coordination and consistency across competent authorities, we analysed the EU NIS directive (Commission, 2025; European Union Agency for Cybersecurity (ENISA), 2023). The European version of the analysed regulation incorporates a Cooperation Group to tackle coordination and consistency issues. The Cooperation Group promotes strategic collaboration and the sharing of information among EU Member States concerning the security of networks and information systems. The EU NIS directives (European Union, 2022) address this gap[3] through *strategic coordination*. In particular, the Cooperation Group serves as a platform for member nations to engage in discussions and coordinate their strategic approaches, with the aim of ensuring consistency across national borders. The EU NIS employs *sharing of best practices*, where the exchange of best practices and knowledge sharing among member states through the group fosters uniformity in cybersecurity strategies and mitigating the inconsistencies in the application of regulations across sectors. The Coordination Group *supports* the development and dissemination of guidance on the implementation of the EU NIS Directives.

To address the inadequate coordination and consistency across competent authorities, the UK NIS should establish a comparable national-level cooperation group. Its main goals will be strategic collaboration, exchange of information, and the sharing of best practices amongst all national competent authorities. The setup could encompass representatives from each designated competent authority, law enforcement, GCHQ, and other pertinent stakeholders. Let us provide some more details of how this gap can be bridged.

1. To enhance compliance monitoring under the UK NIS, we suggest the development of an advanced and centralised digital platform that aggregates regulatory data from all competent authorities (Nooren, Van Gorp, van Eijk, & Fathaigh, 2018). Incorporating AI-based analytics into such a platform could assist in identifying discrepancies, non-compliance patterns, or systemic risks across sectors more efficiently, especially given the scale and heterogeneity of actors involved. Similar AI-supported systems have been used in financial regulation, anti-fraud detection, and public health surveillance (Bughin et al., 2017), demonstrating the potential of AI to improve situational awareness and oversight at scale. While not strictly necessary, these technologies offer promising capabilities that can strengthen regulatory coherence and responsiveness.
2. Another suggestion is the usage of Blockchain technology to ensure transparency and accountability, as it enables the tracking of adherence to regulations (Neisse, Steri, & Nai-Fovino, 2017). By employing blockchain technology, the accuracy and reliability of compliance data can be significantly improved, thereby facilitating effective regulatory oversight.

3.3. Information sharing and analysis

Another identified gap is the lack of focus on the efficiency and efficacy of exchanging and analysing information. The NIS requires GCHQ to communicate, consult, advice, and collaborate with different organisations. However, the success of these operations largely depends on the systems and platforms used for sharing information and analysing it afterwards. Rapid information sharing and good analysis are essential for promptly identifying, responding to, and reducing cyber threats in real-time.

To address the gap in information sharing and analysis, we looked at the model of Information Sharing and Analysis Centers (ISACs) (European Union Agency for Cybersecurity (ENISA), 2024) that have been established in various sectors globally. ISACs are sector-specific entities created to facilitate the sharing of information about cyber threats, vulnerabilities, and incidents among members within a particular sector. They provide a structured mechanism for collecting, analysing, and disseminating actionable threat intelligence among their members, enhancing the sector's overall ability to respond to cyber threats. ISACs has a *sector-specific focus*. By concentrating on specific sectors, ISACs ensures that the information shared is relevant and tailored to the unique needs and challenges of each sector, which can improve the efficiency of cybersecurity measures. Furthermore, ISACs facilitates a collaborative approach to addressing cyber threats, allowing members to benefit from shared experiences, strategies, and response efforts.

To improve information sharing and analysis, the UK NIS can encourage the establishment of sector-specific ISACs or similar information sharing and analysis frameworks. To that end, GCHQ should serve as the national coordination authority overseeing the establishment and

[3] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

operation of sector-specific ISACs. While ISACs would manage their sector-specific operations independently, GCHQ would provide strategic oversight, secure infrastructure, and policy alignment. Specifically, GCHQ could support these efforts by:

1. Facilitating the establishment of ISACs in critical sectors identified under the NIS Regulations.
2. Providing guidance, support, and potential infrastructure for the secure exchange of information.
3. Acting as a bridge between ISACs, international partners, and other relevant entities to ensure comprehensive coverage and response to cyber threats.
4. Incorporating insights gained from ISACs into national cyber threat assessments and strategies.

3.4. Balancing information sharing with privacy and security concerns

Another gap involves the difficulty of maintaining a balance between the requirement of exchanging comprehensive and efficient information and the obligation of safeguarding sensitive information and avoiding any adverse effect on the security or business interests of the involved companies. Although the UK NIS states that information sharing must be relevant, proportionate, and essential, implementing this balance can be intricate. To guarantee that shared information does not unintentionally compromise privacy, security, or business competitiveness, it is necessary to have strong systems in place to classify, process, and share information.

To address this issue we analysed the General Data Protection Regulation (GDPR).[4] The GDPR offers comprehensive guidelines on data protection and privacy for all individuals within the EU and the European Economic Area. It also addresses the transfer of personal data outside these regions. GDPR's principles on data minimisation, purpose limitation, and data protection by design and by default can provide a framework for addressing the balance between information sharing and privacy/security concerns. We analyse below some of the GDPR principles that address the information sharing balance.

- Data Minimisation: The GDPR requires that only data that is essential for the specific purpose of processing is to be retained and processed.
- Purpose Limitation: Data gathered for a certain objective should not be utilised for a different, unrelated objective without obtaining additional consent or having a legal justification. This facilitates the preservation of the accuracy and reliability of information exchange.
- Data Protection by Design and by Default: It refers to the incorporation of data protection measures into the development of business processes for products and services.
- Confidentiality and Security of Processing: The GDPR highlights the significance of safeguarding personal data from unauthorised or unlawful processing, as well as from accidental loss, destruction, or damage.

To address the gap in balancing information sharing with privacy and security concerns, the UK NIS enforcement authorities and relevant stakeholders should adopt GDPR-compliant processes and technologies. For example, by

1. Enforcing rigorous data classification schemes to determine which information can be exchanged and in what specific situations.
2. Creating robust, encrypted communication routes to safeguard data during transmission.
3. Implementing data reduction and purpose limitation principles to guarantee that only essential information is sent to meet the obligations of the NIS Regulations.
4. Performing periodic privacy impact evaluations for information-sharing practices in order to detect and address possible concerns to privacy and security.

3.5. Flexibility and adaptability to emerging threats and technologies

UK NIS capacity to effectively respond to quickly changing cyber threats and developing technology is another issue. The criteria for designating OES (Operators of Essential Services) are static, and the biannual review cycle is not adequate considering the ever-changing nature of cyber risks and the rapid evolution of technology and threat landscapes. Thus, organisations that become crucial as a result of technical advancements or shifts in social dependence are not immediately identified as OES, and regulatory oversight of their cybersecurity practices might consequently be compromised.

In order to fill this gap, we recommend the use of adaptive cybersecurity frameworks that include ongoing monitoring and dynamic risk assessment. An example is the Continuous Diagnostics and Mitigation (CDM)[5] initiative implemented by the United States Department of Homeland Security. The CDM programme offers government departments and agencies the means to continuously discover cybersecurity vulnerabilities, prioritise them according to their possible consequences, and empower cybersecurity specialists to address the most critical issues as a priority. This is done through *continuous monitoring* of cybersecurity risks, *dynamic risk assessments*, and the usage of *automated methods* for detection and response to threats.

To enhance the adaptability of the NIS Regulations to changing cyber threats and technologies, we propose the following implementations.

1. Implement Continuous Monitoring: Revise the regulations to require the ongoing monitoring of cybersecurity risks by both competent authorities and OES, guaranteeing prompt detection and reaction to emerging threats.
2. Dynamic Designation Process: Create a more flexible procedure for the identification of OES, enabling more regular evaluations and modifications to the list of designated organisations, taking into account evolving risk assessments and technological interdependencies.
3. Leverage Automated Tools: Facilitate the adoption of automated cybersecurity solutions among OES to promptly detect, evaluate, and mitigate threats, hence improving their capacity to swiftly respond to incidents.
4. Cross-Sector Collaboration: Enhance cooperation among sectors and competent authorities to exchange information on potential threats and effective strategies, utilising knowledge from other sectors to enhance overall resilience in cybersecurity.

3.6. Dynamic nature of digital services and emerging technologies

Given the static and rigid nature of the UK NIS another gap related to its capacity to adjust to the swiftly changing landscape of digital services and the ongoing introduction of novel technology. NIS stipulates precise activities and considerations for Relevant Digital Service Providers (RDSPs), with a particular emphasis on modern digital services models such as online marketplaces, search engines, and cloud computing. Nevertheless, the rapid rate of advancement in digital services and the emergence of new technologies, e.g., AI, IoTs, can surpass the specific regulations. This results in new services or

[4] https://gdpr-info.eu

[5] https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program

technologies being inadequately regulated or not explicitly addressed by existing guidelines.

In order to understand how to fill that gap, we analysed more flexible and technology-neutral frameworks such as ISO/IEC 27001,[6] which is the global standard for managing information security systems (ISMS). This standard offers a methodical way to effectively manage confidential information to ensure its security. It encompasses the protection of people, processes, and IT systems by implementing a risk management strategy. This standard possesses the ability to adjust and accommodate to emerging security risks, advancements in technology, and alterations in the surrounding conditions. In particular, ISO/IEC 27001 prioritises the administration of information security instead of dictating particular technologies or approaches, allowing it to be flexible for different digital services. It has a risk management process that consistently evaluates the information security risks related to its operations, particularly those arising from new technologies and emerging digital service models, and takes necessary actions to mitigate those risks. ISO/IEC 27001 is based on the concept of ongoing enhancement, necessitating organisations to periodically assess and enhance their ISMS in light of internal audits, incidents, and changing external risks, guaranteeing the long-term effectiveness of security measures.

In order to address the challenge, i.e., keeping up with the fast-paced development of digital services and emerging technologies, we recommend that RDSPs and regulatory authorities should take the following actions:

1. Integrate ISO/IEC 27001 principles: Require RDSPs to implement ISO/IEC 27001 standards for their information security management practices, ensuring an adaptable and strong approach to security that can adjust to emerging threats and technology.
2. Implement a system for regularly reviewing and amending rules to incorporate the most recent advancements in digital services and technologies. This may involve a formal procedure for seeking input from industry experts, technologists, and other relevant parties.
3. Encourage Risk Management Practices: Establish an approach of risk management within RDSPs, highlighting the significance of recognising, evaluating, and minimising risks linked to the delivery of digital services, especially those stemming from emerging technologies.

3.7. International cooperation and compliance

The digital services ecosystem is fundamentally global, with RDSPs occasionally operating in different jurisdictions that have diverse regulatory needs. The UK NIS Regulations prioritise the importance of RDSPs in risk management and reporting serious occurrences to the appropriate authorities. However, it struggles to guarantee adherence to regulations in diverse regulatory environments. Thus, creating disparities in the criteria for reporting incidents, the speed at which responses are provided, and the regulation of the movement of data across borders. These variances can make the response to and handling of cybersecurity incidents having more complex international consequences.

In order to address these challenges, we suggest the implementation of the mechanisms for international collaboration and adherence outlined in the GDPR and the Council of Europe Budapest Convention on Cybercrime. In particular, the use of the GDPR will allow cross-border cooperation mechanisms, as it offers organised procedures for international collaboration, encompassing reciprocal aid and exchange of information among nations. These mechanisms are essential for effectively addressing incidents that impact digital services spanning many jurisdictions. Furthermore, RDSPs can enhance the consistency and efficiency of handling cybersecurity incidents, regardless of their location, by implementing standards for incident reporting and response.

[6] https://www.iso.org/standard/27001

3.8. Specificity and clarity in cybersecurity measures and incident reporting criteria

The UK NIS requires RDSPs to take "appropriate and proportionate measures" to manage risks and to notify authorities of incidents having a "substantial impact". However, the requirements for determining what qualifies as "appropriate and proportionate measures" and a "substantial impact" are generally outlined and may lack the necessary clarity for RDSPs to consistently implement these criteria, creating a gap between the regulations and implementation. This discrepancy can result in diverse interpretations and applications of the regulations, thereby compromising their efficacy in guaranteeing a superior degree of security across all RDSPs.

In order to address this gap, thus, to ensure precise and clear cybersecurity measures and incident reporting, we analyse the NIST Framework and the ISO/IEC 27005 standard for information security risk management. In particular, both guidelines provide extensive guidance on adopting efficient cybersecurity measures, giving RDSPs more precise benchmarks for determining "appropriate and proportionate" actions. RDSPs can enhance their comprehension of incidents that have a "significant impact" and necessitate notice by using the structured incident management and reporting principles outlined in these frameworks. NIST and ISO/IEC 27005 are specifically designed to be regularly updated and adjusted, allowing for RDSPs to consistently align their security policies with the most current threats and optimal methods.

To bridge the gap in specificity and clarity, RDSPs and regulatory bodies should:

1. Adopt and Reference Established Cybersecurity Frameworks: Include explicit mentions of well-established cybersecurity protocols outlined in regulatory guidelines, urging or mandating RDSPs to conform their activities to these benchmarks.
2. Provide Clear Examples and Case Studies: Provide comprehensive instances, case studies, and situations to demonstrate the implementation of "suitable and commensurate actions" and the definition of a "significant influence", aiding RDSPs in gaining a clearer understanding of their responsibilities.
3. Regularly Update Guidance Based on Emerging Threats: Create a systematic procedure to regularly assess and revise cybersecurity protocols and criteria for reporting incidents, taking into account emerging threats and improvements in technology, to ensure continuous relevance and efficacy.

3.9. Discussion: gaps and implementation challenges

As cybersecurity threats continue to evolve, the gaps identified in the UK NIS framework may become even more critical. Emerging attack techniques, such as AI-generated malware, highly targeted ransomware campaigns, and exploitation of Internet of Things (IoT) devices, are expected to intensify the risks faced by supply chains. Without regular updates and adaptive risk management strategies, the static and prescriptive nature of current regulations could leave organisations increasingly vulnerable to new forms of attacks. Thus, regulatory frameworks must be designed with built-in flexibility and periodic revision mechanisms to remain effective against emerging and unforeseen threats.

Implementing the proposed solutions to address these gaps is not without challenges. SMEs, which form a significant portion of supply chains, may face resource constraints that hinder their ability to comply with enhanced security requirements. Larger organisations may encounter operational resistance or face legal complexities when enforcing security obligations across international supply chains. Drawing lessons from industries such as finance and healthcare, which have implemented risk-based, tiered compliance models, one strategy is to introduce scalable security requirements proportionate to the risk

profile and size of the entity. Additionally, public–private partnerships, subsidised cybersecurity support programs for SMEs, and harmonisation of international standards could facilitate more effective and practical adoption of the proposed regulatory enhancements.

4. Security plans and risk assessment for supply chain security

In the previous section, we presented a gap analysis of the UK NIS regulations, where we identified existing solution that can be implemented to bridge these gaps. Our main focus on the UK NIS is on the supply chain cybersecurity and the risks that arise. In this section, we analyse the supply chain security from risk analysis perspective. In particular, we introduce, to the best of our knowledge, the first security plans for each cybersecurity risk profiles for supply chains. This work complements the previous section, which focused on the UK NIS (where suggestions on how to improve the framework were provided), as it provides practical cybersecurity requirements that need to be satisfied by the components of the supply chain.

We start by proposing security plans and their associated security requirements for the supply chain. Identifying the level of risk is an important aspect of the supply chain, as it comes with its own challenges. In this section, we introduce some existing solutions that perform a cybersecurity risk assessment for the supply chain.

4.1. Security plans for supply chain

It is important for companies of a supply chain to define security plans for their suppliers. These plans are composed of security requirements that provide a certain level of guarantee between companies of the supply chain against cyber-attacks in the supply chain. In case security requirements are requested, it is mainly done on a single basis and it is part of the contractual obligations between the involved parties. In order to identify these security requirements, we decided to analyse the security requirements requested by the UK government for their defence suppliers. Our goal is to suggest possible security requirements that general supply chains can ask their companies.

We analysed the Def Stan 05-138 (GOV.UK, 2021) guidance, which is a defence standard that specifies the measures that defence suppliers are required to achieve. In particular, it divides the suppliers into five levels of cyber risk and provides each of them with the requested security requirements.

Cyber risk profiles for supply chains. In the Def Stan 05-138 the companies are divided into five categories regarding their cyber risk profile. We recommend these categories be kept the same also for the cyber risk profile of general supply chain companies. The five categories are provided below:

- **Not applicable**: there is no need for specific cyber control measures, even though, a good practice is to comply with the Cyber Essentials Scheme, when IT systems are used for conducting business.
- **Very low**: the cyber risk is basic and untargeted.
- **Low**: the cyber risks are basic but more targeted, with not persistent attackers that might be semi-skilled.
- **Moderate**: the cyber risks are more advanced, and the attacks are targeted and tailored to get access to an asset(s) or to have a denial of service.
- **High**: the cyber risks are subjective to Advance Persistent Threats (APT) and the attackers are highly sophisticated, organised, well-resourced, and persistent. These attacks may continue for long periods and go unnoticed for months or even years during their initial stages.

Table 2
Security requirements for *Not Applicable* and *Very Low* cyber risk supply chains.

	Strongly recommended	Recommended	Desirable
Not applicable			Comply with the Cyber Essentials Scheme.
Very Low		Comply with the Cyber Essentials Scheme.	

Depending on the category of risk profile that a company has, it needs to comply with specific security requirements. To identify these security requirements, we analysed the requirements provided by Def Stan 05-138, which are very restrictive and sometimes unnecessary when it comes to the general supply chain. They can be used as a starting point for our security requirements of general supply chains. We introduce below the security plans for each of the cyber risk profiles for generic supply chains. In this paper, we introduced three novel categories of implementation for the security requirements: *strongly recommended*, *recommended*, and *desirable* by taking into consideration the level of cyber risk level that generic supply chains have.[7] Furthermore, when appropriate, we also add some further recommendations, mentioned in the below tables as Extra recommendations, (that were not provided in Def Stan 05-138). Except for the *not applicable* and *very low* risk profiles, for the others we divide the security requirements into sic categories, i.e., governance, security culture and awareness, etc. to provide a further level of granularity to our security requirements. Let us now, explain each of the security plans and their requirements.

For the *Not Applicable* and *Very Low* the recommendations are provided in Table 2. Cyber Essential is desirable for *Not Applicable* and recommended for *Very Low*. Please note that Cyber Essentials (National Cyber Security Center (NCSC), 2024) is a certification scheme identifying the minimum steps an organisation should take to protect themselves against cyber risk.

We provide in Table 3 the security recommendations for supply chains with a *Low* level of cybersecurity risk. We divide the security requirements into six categories, plus a seventh (i.e., Extra) where we provide some further requirements. The only strongly recommended requirement for this level is the Cyber Essentials Scheme certificate. Recommended requirements deal with access control policies and defined roles to be put in place, as well as incidents and violations management policies.

In Table 4 the security recommendations for supply chains with a *Moderate* level of cybersecurity risk are provided. The division between the six categories is kept for the *Moderate* as well as the *High* cyber risk requirements. For the *Moderate*, we introduced the Multi-Factor Authentication as a strong requirement, access control policies and back-up recommendations. We also mention risk assessment processes as a desirable requirement. The division of the requirements was made by keeping in mind that we are dealing with general supply chains, where some of the entities involved are SMEs with little resources to be dedicated to security.

Finally, we present in Table 5 the security recommendations for supply chains with a *High* level of cybersecurity risk. Given the *High* risk, we build on top of the *Moderate* requirements, where we strongly recommend back-ups, policies for data loss prevention as well as employee security trainings. IDS and control of traffic flow are desirable. While the availability of critical assets, network monitoring tools, firewalls for critical servers, and security countermeasures are recommended.

[7] For developing our novel security plans, we were based on the requirements provided in the Def Stan 05-138 guidance.

Table 3
Security requirements for *Low* cyber risk supply chains.

	Strongly recommended	Recommended	Desirable
Governance		• Define and implement an information security policy together with the related processes and procedures. • Define and assign information security-relevant roles and responsibilities. • Define and implement a policy about information security risks within the supply chain.	
Security Culture and Awareness		• All functions have sufficient and appropriately qualified resources to manage the establishment, implementation, and maintenance of information security. • Define employee and contractor responsibilities for information security.	• Ensure Information Security training for employees and contractors.
Information Asset Security		• Access control policies for information and information processing facilities.	• Policy for clearly identifying sensitive information.
Info-Cyber Systems Security		• Cyber Essentials Scheme Plus Certification.	• Policy to control the exchanging of information via removable media. • Information technology estate: record and maintain the scope and configuration. • Policy for access rights of users' accounts. • Policy for password confidentiality.
Personnel Security		• Processes to report violations of information security policies.	• Verify credentials of individuals before employment. • Disciplinary process against policy violators.
Security Incident Management		• Incident management policy (detection/resolution/recovery).	
Extra	• Cyber Essentials Scheme certificate.		

4.2. Performing cybersecurity risk assessment in supply chain

In the previous section, we introduced five novel cybersecurity plans (composed of security requirements), one for each risk profile, to improve the supply chain cybersecurity and prevent increasing their risk level. Another important aspect to consider is how the risk assessment is performed by the supply chain. Generally, the cybersecurity risk assessment is performed by a third-party entity or cybersecurity risk experts from the company of the supply chain and requires a certain level of resources to be devoted to this process. Not all companies/entities involved in the supply chain have that level of resources and/or experts. So, it is crucial to identify other solutions for supply chains to perform this risk assessment.

A solution, inspired by the current risk assessment procedure required by the UK MOD (GOV.UK, 2023), is the one where the supply chain companies provide the answers to the cybersecurity risk assessment questionnaire to a governmental body, as a central authority (for example in the UK this body can be NCSC or GCHQ). This solution can work for a limited number of companies or sectors (e.g., defence), but cannot be a reliable one for all types of supply chains, given the enormous amount of companies that might require this service. Furthermore, a good part of SMEs involved in supply chains do not have the right personnel to be able to answer cyber risk assessment questionnaires.

Another solution is the self-risk assessment, performed by the company itself. This solution would remove the centralisation of the cyber risk assessment process, and reduce the resources required to have a third party performing the assessment. Specifically, we envision that risk assessment forms to be provided to the supply chain companies. The risk assessment forms should include a supplier assurance questionnaire, an industry risk assessment (e.g., simpler versions of the following National Cyber Security Center (NCSC) (2020), National Cyber Security Center (NCSC) (2023)), together with *Cyber Implementation Plan* (see the security requirements in Section 4.1). This type of risk assessment should be performed either through an online form and issuing a certificate as an output, or through an online website where the companies have authenticated access and can submit the answers to the various questions, and receive their certificate.

Currently, there are solutions that allow the cybersecurity self-risk assessment for supply chains. For example, the solution introduced in Gokkaya, Aniello, Karafili, and Halak (2024), where a methodology for self-risk assessment for the supply chain is provided. The authors of this paper provide also an online platform[8] that allows supply chain companies to identify their level of interconnected supply chain cybersecurity risk. The methodology employs specific categories of

[8] https://www.securechains.co.uk/login/?next=/

Table 4
Security requirements for *Moderate* cyber risk supply chains.

	Strongly Recommended	Recommended	Desirable
Governance	• Define and implement an information security policy together with the related processes and procedures. • Define and assign information security-relevant roles and responsibilities. • Define and implement a policy about information security risks within the supply chain.	• Put in place policies to detail the employee and contractor responsibilities for information security before granting access to sensitive assets.	• Information security regular reporting.
Security Culture and Awareness		• All functions have sufficient and appropriately qualified resources to manage the establishment, implementation, and maintenance of information security. • Define employee and contractor responsibilities for information security. • Make sure to have information security training for employees and contractors.	• Put in place a repeatable risk assessment process.
Information Asset Security	• Access control policies for information and information processing facilities. • Policy for regular back-up of data off-line and off-site.	• Policy for secure storage, usage, and access of sensitive information. • Put in place a policy for data loss prevention. • Policy for clearly identifying sensitive information.	• Identify asset owners and make sure that asset owners have access to their assets.
Info-Cyber Systems Security	• Cyber Essentials Scheme Plus Certification. • Policy for network monitoring, review computer security event logs for indication of potential incidents. • Policy to monitor user account usage and manage changes of access rights. • Administration access over secure protocols using MFA.	• Policy to control the exchanging of information via removable media. • Policy for access rights of users' accounts. • Policy for password confidentiality. • Undertake risk assessment and management and a policy to assess vulnerabilities (where there are no countermeasures). • Policy to control remote access to networks and systems.	• Policy to control the use of authorised software. • Policy to control the flow of information through network borders.
Personnel Security	• Personnel risk assessment for employees and contractors, check that those responsible for information security have sufficient qualifications and experience.	• Verify the credentials of individuals before employment. • Put in place processes to report violations of information security policies.	• Disciplinary process against employees who violate information security policies or procedures. • Policy for security vetting checks to employees. • Policy to secure organisation assets when individuals cease to be employed in the organisation.
Security Incident Management	• Put in place an incident management policy (detection/resolution/recovery).		

assets, vulnerabilities, and threats that are relevant to most organisations, based on principles outlined in the NIST Framework and insights derived from academic literature. The questionnaire is designed to collect basic information from suppliers without needing them to have extensive knowledge about their cybersecurity posture or the technical complexities of their organisation's assets. The approach aims to calculate cybersecurity risk ratings for each pre-defined threat groups (e.g., software threats) by aggregating the estimates given as answers to the questionnaire. The five levels of risk security used in Gokkaya, Aniello, et al. (2024) can be mapped directly to the five levels of risk provided in Section 4.1. The advantage of this solution is that the user performing the risk assessment does not need to be a security expert, thus, solving the issue of needing security experts in the company performing the self-risk assessment.

Another self-risk assessment solution is the EU Agency for Cybersecurity tool (ENISA, 2024), which is developed for mapping out the network of dependencies and interactions among essential service operators and digital service providers, aligning these with international cybersecurity standards and guidelines. Aimed at assessing the vulnerability due to increased dependency on digital platforms and service providers, which is a key factor in modern supply chains, the tool incorporates indicators aligned with recognised standards including ISO IEC 27002, COBIT5, the NIS Cooperation Group security measures, and the NIST Framework. This facilitates a comprehensive and standardised approach towards assessing and mitigating risks in supply chains.

Other tools are available to assess an organisation's cybersecurity readiness, depending on the specific requirements provided by NIST. These tools cover a broad spectrum of assessments, from comprehensive reviews of cybersecurity programs to targeted evaluations of particular

Table 5
Security requirements for *High* cyber risk supply chains.

	Strongly Recommended	Recommended	Desirable
Governance	• Define and implement an information security policy together with the related processes and procedures. • Define and assign information security-relevant roles and responsibilities. • Define and implement a policy about information security risks within the supply chain.	• Put in place policies to detail the employee and contractor responsibilities for information security before granting access to sensitive assets.	• Information security regular reporting.
Security Culture and Awareness	• All functions have sufficient and appropriately qualified resources to manage the establishment, implementation, and maintenance of information security. • Define employee and contractor responsibilities for information security. • Make sure to have information security training for employees and contractors.	• Put in place a repeatable risk assessment process.	
Information Asset Security	• Access control policies for information and information processing facilities. • Policy for regular back-up of data off-line and off-site. • Policy for secure storage, usage, and access of sensitive information. • Policy for clearly identifying sensitive information.	• Put in place a policy for data loss prevention.	• Identify asset owners and make sure that asset owners have access to their assets.
Info-Cyber Systems Security	• Cyber Essentials Scheme Plus Certification. • Policy for network monitoring, review computer security event logs for indication of potential incidents. • Policy to monitor user account usage and manage changes of access rights. • Administration access over secure protocols using MFA. • Policy for access rights of users' accounts. • Policy for passwords confidentiality. • Undertake risk assessment and management and a policy to assess vulnerabilities (where there are no countermeasures). • Policy to control remote access to networks and systems.	• Policy to control the exchanging of information via removable media. • Policy to control the use of authorised software. • Ensure wireless connections are authenticated. • Deploy network monitoring techniques that complement traditional signature-based detection. • Place application firewalls in front of critical servers to verify and validate the traffic going to the server. • Design networks incorporating security countermeasures, such as segmentation or zoning.	• Policy to control the flow of information through network borders. • Maintain patching metrics and assess patching performance against policy. • Deploy network-based Intrusion Detection System sensors on ingress and egress points within the network and update regularly with vendor signatures. • Define and implement a policy to control installations of any changes to software on any systems on the network. • Control the flow of traffic through network boundaries and police content by looking for attacks and evidence of compromised machines. • Ensure Data Loss Prevention at egress points to inspect the contents of information and take appropriate action to prevent its inadvertent or malicious release.
Personnel Security	• Personnel risk assessment for employees and contractors, check that those responsible for information security have sufficient qualifications and experience.	• Verify the credentials of individuals before employment. • Put in place processes to report violations of information security policies. • Policy to secure organisation assets when individuals cease to be employed in the organisation.	• Disciplinary process against employees who violate information security policies or procedures. • Policy for security vetting checks to employees.
Security Incident Management	• Put in place an incident management policy (detection/resolution/recovery).	• Proactively verify security controls are providing the intended level of security. • Define and implement a policy to ensure the continued availability of critical asset(s)/information during a crisis.	

areas. The Axio Cybersecurity Programme Assessment Tool[9] is another resource that allows organisations to measure their cybersecurity preparedness against recognised standards. The Baldrige Cybersecurity Initiative tool[10] combines the thoroughness of their proposed framework with the NIST Framework. By aligning cybersecurity risk management with larger organisational objectives, this solution enhances operational preparedness while improving cyber health. The Cyber Security Evaluation tool (CSET)[11] developed by the US Department of Homeland Security provides a thorough assessment of compliance with many standards, including the NIST Framework. CSET offers an analysis of an organisation's cybersecurity procedures, identifying weaknesses and suggesting strategies to enhance security.

Another interesting problem is how the result of the cybersecurity risk assessment can be shared with the supply chain. Once the "certificate" about the level of risk is released, then a possibility is to make this information available to the public. This option will make companies that have medium or higher risk targets for future cyberattacks. Instead, other solutions might be the sharing of a digital signed certificate with the suppliers, or the usage of a portal where the company can share their certificate together with the cybersecurity plan in secure and safe manner.

5. Supply chain contracting about data and information sharing

Supply chain contracts are legally binding agreements between two or more parties involved in the production, distribution, or sale of goods or services within a supply chain network (Coltman, Bru, Perm-Ajchariyawong, Devinney, & Benito, 2009; Katok & Wu, 2009; Wang, 2002). These contracts help establish the terms and conditions under which the parties agree to conduct their business relationships and play a crucial role in establishing clear expectations, minimising risks, and ensuring smooth coordination among the various stakeholders involved in the supply chain process (Kremer & C Schneeweiss, 2006). The supply chain contract design typically includes the parties involved in the supply chain process, terms and conditions of the agreement, roles and responsibilities, risk management and allocation, resolution of disputes, and compliance with regulations and clauses signed by the parties. Recently the supply chain contracts have been enhanced with features relevant to confidentiality clauses, intellectual property rights, information sharing, and security clauses as well as how the data and information are shared among the parties involved and how secure is the technological infrastructure for the transmission of such data and information (Agrawal, Angelis, Khilji, Kalaiarasan, & Wiktorsson, 2023; Omar, Jayaraman, Salah, Debe, & Omar, 2020).

Supply chain contracts and information security are intimately linked due to the sensitive nature of data exchanged and the potential risks associated with sharing information across supply chain networks (Chen & Özer, 2019; Liu, Jiang, Feng, & Chin, 2020). Information security within supply chain contracts involves protecting confidential data, mitigating cybersecurity threats, and ensuring compliance with relevant regulations (Williams, Lueg, & Lemay, 2008; Williams, Ponder, & Autry, 2009).

Information security can be ensured through the supply chain contract design in various levels that protect all the parties involved, provide liability clauses and risk management measures, but also ensure the secure transmission of data and the maintenance of the technology among the contracting parties (Williams et al., 2009). Initially, the supply chain contract should contain specific data protection and privacy requirements that all parties must adhere to when handling personal or sensitive data throughout the procurement process or other supply chain steps. This may include compliance with regulations such as the GDPR or the California Consumer Privacy Act. Information sharing among supply chain partners should also be defined when the contract is established. The supply chain contract should include the types of data that can be shared, the methods of transmission, and the security measures that must be implemented to safeguard the data during transit and storage (Fawcett, Osterhaus, Magnan, Brau, & McCarter, 2007; Ha & Tong, 2008; Zhang & Chen, 2013; Zhou & Benton, 2007). Supply chain contracts often include clauses relevant to confidential information and explain specifically how sensitive information shared between parties will be handled. This includes provisions for protecting trade secrets, proprietary technology, customer data, financial information, and other confidential data.

Another important aspect that should be highlighted in the contracts should include provisions for vendor risk management, where suppliers and other third-party vendors are required to demonstrate compliance with information security requirements and undergo periodic assessments to evaluate and provide proof for their security posture (Pettit, 2008; Williams et al., 2009). As mentioned in previous parts of the paper, there should be safeguarding measures explained in the contracts relevant to cybersecurity standards and controls to protect against data breaches, unauthorised access, malware attacks, and other cybersecurity threats. This may include implementing encryption, access controls, firewalls, intrusion detection systems, and regular security audits.

Finally, supply chain contracts may also include directions about incident response and notification in cases of security breaches, guidelines about regular controls and audits, but also how to terminate or transfer the contract to a new vendor in cases of security breaches. These procedures include compliance monitoring to ensure that all parties are meeting their information security obligations. Supply chain contracts should foster in a stronger manner the security provisions, provide guidelines to organisations for risk mitigation, protect sensitive data, and provide trust and confidence among supply chain partners and customers.

6. Conclusion and future work

The main goal of this work is to improve and strengthen the cybersecurity in supply chains. In particular, we worked in different directions to reach our goal, by focusing on the UK NIS Regulations (Legislation.gov.uk, 2018) and its existing infrastructure around supply chain security.

We started by identifying the critical gaps of the UK NIS that, if addressed, could significantly increase the effectiveness of the framework in protecting against cyber threats. These gaps cover various aspects of cybersecurity management, such as implementation and metrics, coordination and information sharing, finding a balance between information protection and sharing, adaptability to evolving threats, international cooperation and compliance, and regulatory specificity. For each of the gaps we provided solutions taken from other existing frameworks or technologies, and how these solutions could be implemented. Our gaps analysis and proposed solutions benefit not only the UK NIS framework improvement, but also the enhancement of other existing frameworks.

Our second contribution is more general to supply chain security, where we introduce novel security requirements for each of the risk profiles, with a focus on the UK cyberspace. These requirements can be applied to every type of supply chain in the UK, but can be easily adapted to supply chains in other countries. We continued our analysis by identifying solutions for cybersecurity risk assessments, with an emphasis on self-assessment solutions. The above are more regulatory and technical solutions, which sometimes are difficult to enforce. This is why, we also analysed how supply chain contracting can be used as a powerful tool to improve the security and privacy of data and information sharing.

[9] https://learn.axio.com/free-tool

[10] https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

[11] https://www.nist.gov/cyberframework/assessment-auditing-resources

There are different interesting future work directions. In the area of risk assessment, it would be interesting to integrate the results of the risk assessments in more formal tools (Cristani, Karafili, & Viganò, 2012, 2014) that help the prediction of risk as well as the preventive and mitigative actions to take. Another interesting area of future work is the usage of AI. Future cybersecurity risk assessments should address AI's potential to automate tasks while mitigating privacy risks. For example, incorporating AI-driven solutions for real-time monitoring and feedback (Mohammed & Aljanabi, 2024) to risk assessment, can drastically improve the security of supply chains. Another interesting approach, in combination with AI-driven solutions, is the usage of behavioural analytics (Amirthayogam et al., 2024), which can act as a complementary approach to traditional risk assessment frameworks.

Moreover, a longitudinal study evaluating the adoption and long-term effectiveness of the proposed cybersecurity solutions, including the security plans and self-risk assessment methods introduced in this paper, would be a valuable research contribution. Tracking organisations over time would allow for a deeper understanding of how supply chain cybersecurity evolves, how compliance and risk levels change, and which practices sustain resilience against emerging threats. Another interesting research direction is the analysis of risk interdependencies among supply chain members. An extended, dependency-aware risk model would enable more precise risk assessments and support the development of effective countermeasures.

Future research should also focus on empirical validation of the proposed risk assessment plans and self-assessment models. This could include pilot studies within industry supply chains or simulation-based evaluations to measure improvements in risk management, compliance, and supplier accountability.

In addition to these directions, it is also important to explore how emerging technologies like blockchain and advanced IoT networks impact supply chain cybersecurity. Blockchain can enhance transparency, integrity, and trust but also brings new security and privacy risks that regulators must address. Likewise, the growing use of IoT devices expands attack surfaces, demanding new security and risk mitigation strategies.

CRediT authorship contribution statement

Betul Gokkaya: Writing – original draft, Methodology, Investigation, Conceptualization. **Konstantina Spanaki:** Writing – original draft, Methodology, Investigation, Conceptualization. **Erisa Karafili:** Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Investigation, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

The author is an Editorial Board Member/Editor-in-Chief/Associate Editor/Guest Editor for this journal and was not involved in the editorial review or the decision to publish this article.

Acknowledgments

This work was partially supported by the UK Department for Science, Innovation and Technology.

References

Agrawal, T. K., Angelis, J., Khilji, W. A., Kalaiarasan, R., & Wiktorsson, M. (2023). Demonstration of a blockchain-based framework using smart contracts for supply chain collaboration. (Accessed 14 January 2025).

AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (smes): A meta-analysis approach. *Electronics*, *12*(17), 3629.

Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021). Solar winds hack: In-depth analysis and countermeasures. In *2021 12th international conference on computing communication and networking technologies* (pp. 1–7). IEEE.

Amirthayogam, G., Kumaran, N., Gopalakrishnan, S., Brito, K. A., S., RaviChand, & Choubey, S. B. (2024). Integrating behavioral analytics and intrusion detection systems to protect critical infrastructure and smart cities. *Babylonian Journal of Networking*, *2024*, 88–97.

Bughin, J., Hazan, E., Ramaswamy, S., Chu, M., Allas, T., Dahlström, P., et al. (2017). *Artificial intelligence the next digital frontier*. McKinsey & Company.

Chen, Y., & Özer, Ö. (2019). Supply chain contracts that prevent information leakage. http://dx.doi.org/10.1287/mnsc.2018.3200, (Accessed 14 January 2025).

Coltman, T., Bru, K., Perm-Ajchariyawong, N., Devinney, T. M., & Benito, G. R. G. (2009). Supply chain contract evolution. http://dx.doi.org/10.1016/j.emj.2008.11.005, (Accessed 14 January 2025).

Commission (2025). NIS2 directive: new rules on cybersecurity of network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. (Accessed 02 February 2025).

Cristani, M., Karafili, E., & Viganò, L. (2012). Towards a logical framework for reasoning about risk. In G. Quirchmayr, J. Basl, I. You, L. Xu, & E. Weippl (Eds.), *Multidisciplinary research and practice for information systems* (pp. 609–623).

Cristani, M., Karafili, E., & Viganò, L. (2014). Tableau systems for reasoning about risk. *J Ambient Intell Human Comput*, *5*, 215–247. http://dx.doi.org/10.1007/s12652-013-0186-7.

ENISA (2024). ENISA publishes a tool for the mapping of dependencies to international standards. https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-a-tool-for-the-mapping-of-dependencies-to-international-standards. (Accessed 14 January 2025).

European Union (2022). 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 repealing directive (eu) 2016/1148. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN . (Accessed 14 January 2025).

European Union Agency for Cybersecurity (ENISA) (2023). NIS directive: Overview and implementation. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new, .(Accessed 14 January 2025).

European Union Agency for Cybersecurity (ENISA) (2024). Information sharing and analysis centers (isacs). https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing. (Accessed 25 March 2024).

Fawcett, S. E., Osterhaus, P., Magnan, G. M., Brau, J. C., & McCarter, M. W. (2007). Information sharing and supply chain performance: the role of connectivity and willingness. http://dx.doi.org/10.1108/13598540710776935, (Accessed 14 January 2025).

Gokkaya, B., Aniello, L., Karafili, E., & Halak, B. (2024). A methodology for cyber-security risk assessment in supply chains. In *Computer security. ESORICS 2023 international workshops* (pp. 26–41). Springer Nature Switzerland.

Gokkaya, B., Karafili, E., Aniello, L., & Halak, B. (2024). Global supply chains security: a comparative analysis of emerging threats and traceability solutions. *Benchmarking: An International Journal*.

GOV. UK (2021). Cyber security for defence suppliers (def stan 05-138). https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138. (Accessed 14 January 2025).

GOV. UK (2022). Defence condition 658: cyber (flow-down). https://www.gov.uk/government/publications/defence-condition-658-cyber-flow-down. (Accessed 14 January 2025).

GOV. UK (2023). Defence cyber protection partnership. https://www.gov.uk/guidance/defence-cyber-protection-partnership. (Accessed 14 January 2025).

Greenberg, A. (2018). The untold story of notpetya, the most devastating cyberattack in history. *Wired*, *22*.

Ha, A. Y., & Tong, S. (2008). Contracting and information sharing under supply chain competition. http://dx.doi.org/10.1287/mnsc.1070.0795, (Accessed 14 January 2025).

Katok, E., & Wu, D. Y. (2009). Contracting in supply chains: A laboratory investigation. http://dx.doi.org/10.1287/mnsc.1090.1089, (Accessed 14 January 2025).

Kremer, M., & C Schneeweiss, M Zimmermann (2006). On the validity of aggregate models in designing supply chain contracts. http://dx.doi.org/10.1016/j.ijpe.2005.12.007, (Accessed 14 January 2025).

Legislation. gov. uk (2018). The network and information systems regulations. *2018*, (506), https://www.legislation.gov.uk/uksi/2018/506/made, . (Accessed 14 January 2025).

Liu, H., Jiang, W., Feng, G., & Chin, K. S. (2020). Information leakage and supply chain contracts. http://dx.doi.org/10.1016/j.omega.2018.11.003, (Accessed 14 January 2025).

Mohammed, S. Y., & Aljanabi, M. (2024). Advancing translation quality assessment: Integrating ai models for real-time feedback. *EDRAAK*, *2024*, 1–7.

National Cyber Security Center (NCSC) (2020). Supplier assurance questions. https://www.ncsc.gov.uk/guidance/supplier-assurance-questions. (Accessed 14 January 2025).

National Cyber Security Center (NCSC) (2023). Risk management. https://www.ncsc.gov.uk/collection/risk-management/the-fundamentals-and-basics-of-cyber-risk. (Accessed 14 January 2025).

National Cyber Security Center (NCSC) (2024). Cyber essentials. https://www.ncsc.gov.uk/cyberessentials/overview. (Accessed 14 January 2025).

National Institute of Standards and Technology (NIST) (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. (Accessed 14 January 2025).

Neisse, R., Steri, G., & Nai-Fovino, I. (2017). A blockchain-based approach for data accountability and provenance tracking. In *Proceedings of the 12th international conference on availability, reliability and security* (pp. 1–10).

Nooren, P., Van Gorp, N., van Eijk, N., & Fathaigh, R. Ó. (2018). Should we regulate digital platforms? a new framework for evaluating policy options. *Policy & Internet*, *10*(3), 264–301.

Omar, I. A., Jayaraman, R., Salah, K., Debe, M., & Omar, M. (2020). Enhancing vendor managed inventory supply chain operations using blockchain smart contracts. http://dx.doi.org/10.1109/ACCESS.2020.3028031, (Accessed 14 January 2025).

Pettit, T. J. (2008). Supply chain resilience: Development of a conceptual framework, an assessment tool and an implementation process. *Security*, (Accessed 14 January 2025).

Schauer, S., Polemi, N., & Mouratidis, H. (2019). Mitigate: a dynamic supply chain cyber risk assessment methodology. *Journal of Transportation Security*, *12*, 1–35.

Spanaki, K., Karafili, E., & Despoudi, S. (2022). Digital architectures: frameworks for supply chain data and information governance. In D. Ivanov B. L. MacCarthy (Ed.), *The digital supply chain* (pp. 147–161). Elsevier, http://dx.doi.org/10.1016/B978-0-323-91614-1.00009-5.

Wang, C. X. (2002). A general framework of supply chain contract models. http://dx.doi.org/10.1108/13598540210447746, (Accessed 14 January 2025).

Williams, Z., Lueg, J. E., & Lemay, S. A. (2008). Supply chain security: An overview and research agenda. http://dx.doi.org/10.1108/09574090810895988, (Accessed 14 January 2025).

Williams, Z., Ponder, N., & Autry, C. W. (2009). Supply chain security culture: Measure development and validation. http://dx.doi.org/10.1108/09574090910981323, (Accessed 14 January 2025).

Zhang, J., & Chen, J. (2013). Coordination of information sharing in a supply chain. http://dx.doi.org/10.1016/j.ijpe.2013.01.005, (Accessed 14 January 2025).

Zhang, Y., & Guin, U. (2019). End-to-end traceability of ics in component supply chain for fighting against recycling. *IEEE Transactions on Information Forensics and Security*, *15*, 767–775.

Zhou, H., & Benton, W. C. (2007). Supply chain practice and information sharing. http://dx.doi.org/10.1016/j.jom.2007.01.009, (Accessed 14 January 2025).