Towards a Cybersecurity Awareness Governance Framework for SMEs

Edoardo Carlini[1], Erik Bergström[1,*] and Joakim Kävrestad[1]

[1]Jönköping University, School of Engineering, Computer Science and Informatics.

Abstract

Small and medium enterprises (SMEs) account for over 90% of businesses worldwide, yet they remain disproportionately vulnerable to cyberattacks. A recurring problem is that cybersecurity awareness is often treated as an employee training issue rather than a governance responsibility. Existing standards and frameworks, including NIST CSF 2.0, ISO 27001, NIS2, and ENISA guidance, provide important governance, regulatory, technical, and capability-oriented support. However, their breadth and implementation demands can still create barriers for resource-constrained SMEs, and the literature lacks a lightweight procedural framework focused specifically on board-level governance of cybersecurity awareness. Following a Design Science Research methodology grounded in a literature review and preliminary expert feedback, this paper develops a Cybersecurity Awareness Governance framework for SMEs. The framework consists of seven phases that guide boards and senior decision-makers from company profiling and regulatory mapping, through board-level accountability, maturity assessment, role structuring, and role-tailored training, to continuous monitoring and organisational learning. The framework synthesises previously published models, including the Five Lines of Accountability, the CICGM maturity model, and the CARE and KAB measurement frameworks, into an accessible governance process. The proposed framework is positioned as a lightweight, CSA-specific governance layer that can help SMEs establish the awareness, accountability, and organisational conditions needed to make effective use of broader cybersecurity standards and maturity-focused tools.

Keywords

Cybersecurity awareness, cybersecurity governance, SME, governance framework, Design Science Research, Board of Directors, security awareness training

1. Introduction

In recent years, small and medium enterprises (SMEs) have been increasingly targeted by cyberattacks. One reason for this is that many SMEs lag behind in cybersecurity, both in terms of training and awareness and of having the tools and software to defend themselves and identify data breaches [1, 2, 3]. At the same time, accelerated digitalisation has increased SMEs' exposure to cyber risks and, as a consequence, many enterprises have struggled to keep pace with the cybersecurity implications of this change [4, 5]. A consistent finding across industry reporting is that a large proportion of data breaches involve a human element, whether through error or social engineering, with phishing among the most common entry points [6].

Cybersecurity awareness (CSA) refers to the knowledge, attitudes, and behaviours that individuals and organisations exhibit to protect digital assets, information systems, and personal data from cyber threats [3, 7]. Awareness directs attention to security issues, helps individuals perceive potential implications, and supports responsible decision-making [3, 7]. While CSA is widely discussed in the literature, the governance of CSA remains underdeveloped, particularly regarding how awareness is initiated, sustained, and managed at the organisational level [8].

The importance of this gap lies in the fact that no employee training programme, technical control, or procedural framework is likely to be consistently adopted or sustained without a clear governance approach from the board, even where regulatory obligations exist [3, 8]. Governance refers to the

The 12th International Conference on Socio-Technical Perspectives in IS (STPIS'26), September 16–17, 2026, L'Aquila, Italy.
*Corresponding author.
caed25hk@student.ju.se (E. Carlini); erik.bergstrom@ju.se (E. Bergström); joakim.kavrestad@ju.se (J. Kävrestad)
0009-0006-8683-2538 (E. Carlini); 0000-0002-1436-2980 (E. Bergström); 0000-0003-2084-9119 (J. Kävrestad)
© 2026 CC-BY logo & © 2026 Copyright for this paper by its author(s). Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073
published 2026-11-19

CEUR-WS.org/Vol-4334/paper14.pdf

decision-making methods and strategic direction through which the management team runs the company. In a cybersecurity context, it encompasses the policies and actions put in place to protect the organisation and respond to potential attack scenarios [1]. CSA governance can therefore be described as the responsibilities and practices through which executive management provides strategic direction, ensures that objectives are met, manages activities appropriately, and supports responsible resource use to enhance cybersecurity [9]. However, these definitions do not specify the procedural sequence through which board members should enact CSA governance: from understanding the organisation's risk profile, through establishing accountability structures and complying with laws and regulations, to designing and sustaining a CSA programme. This procedural gap is what the present paper aims to address.

Board members may be held accountable for cybersecurity measures and their consequences in the event of a data breach, yet they often lack the knowledge and tools needed to support cybersecurity decision-making [10]. SME board members also tend to underestimate the consequences of being hacked, assuming that an incident mainly involves data theft, when consequences can include operational disruption, fraud, reputational damage, regulatory penalties, and potential business closure [11, 12]. Mumford [13] argued that rapidly changing technological environments can challenge traditional organisational approaches to problem-solving and decision-making, creating a need for governance processes capable of responding to new and evolving threats.

Several factors explain this situation. Board engagement with cybersecurity is often driven primarily by regulatory obligations and the direct experience of having suffered a cyberattack, whereas preventive motivators remain comparatively weak [8]. This suggests that SME governance bodies tend to behave reactively rather than proactively. Although established standards and frameworks such as ISO 27001 [14], NIST CSF 2.0 [15], NIS2 [16], and ENISA guidance [17] provide substantial support, SMEs may still face difficulties operationalising them because of resource constraints, limited in-house expertise, and implementation complexity [3, 12]. The classic perception of cybersecurity as the sole responsibility of the CISO or ICT department also persists, despite its implications across the organisation [2].

The aim of this paper is to synthesise the current state of SME cybersecurity awareness governance [3, 18] and to develop a framework that guides board members in governing CSA across their organisation in a simpler, more accessible way, given the regulatory complexity and practical challenges they face compared to those of larger organisations. Rather than addressing technical cybersecurity implementation, this framework targets the governance layer, equipping SME decision-makers with an understanding of their exposure, responsibilities, and legal obligations, and providing them with a structured process to embed CSA governance into their business processes [1]. The framework is intended to be sector-independent [19], as the governance and awareness gaps it addresses are general rather than industry-specific, and it refers to established standards including ISO 27001, NIST CSF 2.0, NIS2, and ENISA guidelines to support regulatory alignment and practical relevance.

2. Related Work and Problem Analysis

The European Commission defines SMEs as enterprises with fewer than 250 employees and either an annual turnover not exceeding €50 million or an annual balance-sheet total not exceeding €43 million [20]. SMEs are crucial to the global economy, accounting for more than 90% of businesses worldwide [11]. Their limited resources, lack of specialised personnel, and the difficulty in adopting complex cybersecurity frameworks make them particularly exposed to cybersecurity risks [12]. Cyberattacks can therefore have severe consequences for SMEs, including financial losses, operational disruption, reputational damage, and recovery challenges [21]. Another recurring issue is the "one size fits all" approach to cybersecurity: many available products and frameworks are standardised and do not fit SMEs' heterogeneous needs, leaving them insufficiently protected [12].

CSA encompasses the knowledge, attitudes, and behaviours that enable individuals and organisations to recognise cyber threats, understand their implications, and respond to them appropriately [3, 7]. It extends beyond technical knowledge and includes, e.g., the capability to make conscious security

decisions during daily operations. While the concept is well established in the literature, its practical implementation remains challenging, particularly given the central role human error increasingly plays in cybersecurity incidents [5, 22]. The COM-B model (Capability, Opportunity, Motivation–Behaviour) [23] provides a behavioural perspective for understanding why awareness alone may not result in secure behaviour. It conceptualises behaviour as arising from the interaction between individuals' capabilities, opportunities in their environment, and motivation. Although COM-B is not used directly as a design component in the proposed framework, it illustrates the broader awareness–behaviour gap that the framework must address.

Human error is often seen as one of the most significant threats to SME cybersecurity. The 2024 Verizon Data Breach Investigations Report found that 68% of breaches involved a non-malicious human element, such as a person falling victim to social engineering or making an error [6]. Another report found that human error was a contributing factor in 85% of data breaches [1]. These incidents stem from behavioural and awareness gaps rather than purely technical failures; employees frequently lack awareness and understanding of the risks associated with common behaviours such as opening suspicious emails, downloading malicious attachments, or using weak passwords [24]. This points to another recurring problem: CSA training does not automatically translate into secure behaviour, as people may still make mistakes despite knowing recommended practices [25, 26].

Research has consistently shown that, despite technological advancements in security systems, human mistakes remain a critical vulnerability that no purely technical solution can eliminate [3, 5, 27]. To address this problem, CSA training is needed to strengthen employees' awareness, judgement, and security-related behaviour. Traditional CSA training methods typically consist of seminars, lectures, generic online courses, and short tests. While such methods may increase knowledge, they often have a limited effect on lasting behavioural change: employees may forget the material, fail to connect it to their daily work practices, or treat it as a compliance exercise rather than as practical security guidance [7, 26].

More recent approaches have therefore shifted towards interactive and role-tailored learning methods, including gamification, simulated phishing campaigns, contextual exercises and real-time feedback mechanisms. These approaches can make training more relevant to employees' actual work contexts and support the development of practical skills that can be applied during daily operations [25, 7]. Rather than treating employees only as the weakest link in the security chain, such approaches aim to strengthen their ability to recognise, report, and respond to threats, particularly phishing and other forms of social engineering [28, 7].

To further improve the effectiveness of CSA training, organisations increasingly need continuous and personalised learning processes. In a rapidly evolving threat landscape, employees are repeatedly exposed to new kinds of threats; consequently, awareness activities must be updated and adapted over time. Personalised and adaptive training approaches, tailored to employees' knowledge gaps, roles, and risk exposure, are therefore more suitable than generic one-size-fits-all approaches, especially when they are combined with mechanisms for monitoring outcomes and adjusting the programme accordingly [3, 7].

However, the effectiveness of any training ultimately depends on the governance structure that enables and manages it. Without company commitment to CSA as a strategic priority and investment in it, even the best training programme is unlikely to be sustained without adequate support [8, 3]. This is consistent with the socio-technical perspective underlying Mumford's ETHICS approach [29], according to which technical arrangements should be considered together with organisational structures, human needs, and work practices.

2.1. Cybersecurity awareness in SMEs

Despite the recognised importance of CSA training, its adoption among SMEs remains limited. A 2021 survey found that only 19% of SMEs in the European Union had offered cybersecurity training in the previous year [3]. A survey of 141 UK-based SMEs conducted by Erdogan et al. [18] found that, despite 80% of respondents reporting moderate to high cybersecurity awareness, only 19% confirmed that their

organisation provided cybersecurity training to employees. This discrepancy indicates a substantial gap between self-reported cybersecurity awareness and the provision of formal cybersecurity training, with potential implications for governance. The same UK survey found that, among the SMEs that provided cybersecurity training, the content primarily covered basic security and privacy topics and was typically delivered when employees joined the organisation, with some companies repeating the training annually [18]. Similar challenges have been identified in the manufacturing sector, where improving cybersecurity awareness among SMEs requires approaches tailored to employees' work contexts and organisational conditions [30]. The 2017 Ponemon Institute SME study reinforces this picture, finding that 54% of participants attributed data breaches in their organisations to negligent employees [3], yet these organisations did not invest in CSA training to prevent such incidents. These findings illustrate a recurring disconnect between recognising human-related cybersecurity risks and investing in measures intended to address them. Research on SMEs further shows that the adoption of awareness-raising activities is shaped by resource constraints, ease of implementation, content quality, adaptability, comprehensibility, compliance tracking, management support, and employee motivation [31]. These findings reinforce the view that CSA adoption in SMEs is an organisational and managerial challenge.

Several factors explain why CSA remains ungoverned in most SMEs. In many cases, board members lack the foundational knowledge of cybersecurity to evaluate whether awareness programmes are needed, let alone to determine which ones are appropriate for their organisation's risk profile [8, 12]. Without this governance-level understanding, decisions about investing in training are either postponed indefinitely or delegated to IT staff who lack the strategic authority to secure sustained funding and plan the programme effectively [8]. The problem is also compounded by a supply-side gap: organisational IT security research has long neglected the SME context, partly because SME cybersecurity has often been perceived as of limited interest and low return on investment. This has produced frameworks and guidance tailored to large enterprises that are not suited for smaller organisations, thereby leaving SME boards without accessible tools to inform their governance decisions [3, 18].

Given the increasing frequency and complexity of cyber threats, security awareness training must be a priority for SMEs, which have become attractive targets precisely because of their limited resources and less robust infrastructure [32, 33]. It is therefore essential that they have not only the right training tools but also the support of governance structures and guidance necessary to deal with these threats. Research in the broader corporate-governance literature indicates increasing attention to board-level cybersecurity oversight [34], although this evidence does not specifically concern SMEs. This reinforces the need to examine how such governance can be operationalised in the SME context.

2.2. Governing cybersecurity awareness

The gap between the recognised importance of CSA and its actual adoption in SMEs points to a structural deficit in the tools, procedures, frameworks, and software available for this segment, particularly regarding budget, workforce size, and time constraints [3]. Unlike many large enterprises, SMEs often lack the resources to maintain specialised cybersecurity personnel and comprehensive in-house security capabilities [21, 35]. Documentation must also be relevant and meaningful, since vague or overly standardised text can add complexity rather than support use [34].

Kappe [12] found that most SMEs' awareness gaps stem partly from not consulting publicly available cybersecurity material at all, and that even among those who did, 55% did not understand it. Companies often consider basic information security measures, such as backups, redundancy, and antivirus software, to be sufficient protection against attacks, when in reality they are not [12]. This highlights both the importance of expert consultation and the need to make cybersecurity documentation more accessible to non-professionals.

Although established cybersecurity standards, frameworks, and regulatory instruments such as ISO 27001, NIST CSF 2.0, and NIS2 provide substantial guidance, SMEs may face difficulties operationalising them because of limited resources, specialised expertise, and implementation capacity [3, 12].

2.3. Governance and operational barriers

Seven recurring governance-related obstacles were identified through the literature review and used to inform the framework design (see Section 3 for details on the method):

Absence of governance-level awareness. The literature consistently shows that SME board members often lack a foundational understanding of cybersecurity risks, their regulatory obligations, and the consequences of failing to act [3, 11, 12]. This is not merely a knowledge gap about technical threats but a governance gap: decision-makers do not recognise CSA as a subject that falls within their strategic responsibilities. As a result, cybersecurity is often delegated to IT personnel, who often lack formal training themselves [12]. Gale et al. found that board members either avoided cybersecurity topics due to their lack of knowledge or loaded all responsibility onto specific members perceived to have the requisite expertise [8].

Underestimation of exposures and consequences. SME board members consistently underestimate both the likelihood and the severity of cyberattacks. Many assume that the consequences of a breach are limited to data theft, failing to account for operational disruption, reputational damage, regulatory penalties, and the potential for business closure [11, 12].

Lack of economic and strategic motivation. The literature suggests that SME boards are most likely to engage with cybersecurity when they need to meet regulatory or professional expectations, or after they have experienced a cyberattack. Consultants and pressure to imitate other organisations appear to be weaker motivators [8]. This suggests that SME governance bodies are reactive rather than proactive in their approach to cybersecurity awareness. Without a structured mechanism to make the economic case for CSA, including quantified risk exposure, potential regulatory fines, and insurance implications, as well as market-sector requirements, the board lacks the strategic motivation to act [36].

Absence of a governance framework tailored to SMEs. Although well-established frameworks, standards, regulatory instruments, and guidance such as NIST CSF 2.0, ISO 27001, NIS2, and ENISA guidelines exist, SMEs may face difficulties operationalising them because of limited resources, specialised expertise, and implementation capacity [12, 3]. Although these frameworks include governance components, the literature reviewed here suggests that they do not provide a dedicated, lightweight procedural approach focused specifically on governing CSA at the board level in SMEs. Kappe et al. [12] found that most SMEs do not consult publicly available cybersecurity materials at all, and among those who did, 55% did not understand them. This gap is not limited to the SME context: an analysis across five databases found that, while country-specific solutions exist, no general cybersecurity governance framework has been established, with the literature skewed towards management rather than governance [37].

Failure to integrate CSA into the business plan. A recurring finding is that CSA and secure operations are treated as stand-alone activities, like a training session or a compliance checkbox, rather than being embedded into the organisation's strategic planning and daily operations [11, 34]. This separation means that, even when awareness initiatives exist, they are not embedded in daily operations. They also lack governance support, sustained funding, and organisational accountability; therefore, they are unlikely to produce lasting behavioural changes.

Disconnection between IT reporting and board comprehension. There is also a communication gap between IT/security personnel and the board. IT departments often struggle to present cybersecurity information in terms that are meaningful for governance decision-making because no shared reporting format has been agreed upon, while boards lack the baseline knowledge required to understand and interpret technical reports [8]. Aleem et al. [38] examined a related organisational disconnect between physical and information-security functions and proposed a converged security approach to improve coordination. Their work illustrates how differences in responsibilities, terminology, and organisational structures can impede shared understanding across security functions. This disconnection results in governance decisions being made without an adequate understanding of the organisation's needs or the actual security posture. Furthermore, IT personnel lack the strategic direction they need to prioritise their efforts effectively. This is supported by practitioner survey data: 58% of CISOs report difficulty communicating cybersecurity risk to the board in business terms, and 53% believe their priorities are

not fully aligned with senior leadership [39].

Awareness-behaviour gap. The literature indicates that greater security awareness does not necessarily translate into correspondingly secure behaviour [5]. This has direct governance implications: delivering awareness training is necessary but not sufficient. Governance must also create organisational conditions, such as accountability structures, cultural norms, and measurement mechanisms, that enable awareness to translate into sustained behavioural change and for best practices to be embedded in daily operations [7, 34]. Sadok et al. [40] show how employees may perceive security requirements as obstacles to their primary work and may circumvent them when security practices are poorly integrated into everyday workflows. This reinforces the need to embed CSA within organisational practices rather than treating it as a separate compliance activity.

3. Research Method and Framework Development

The research followed the Design Science Research (DSR) process adapted from Vaishnavi and Kuechler (2015) [41]. This method provided a structured and systematic approach for developing and evaluating a design artefact against the problems identified in the previous section. The DSR process structured the research into five distinct phases: awareness of the problem, suggestion, development, evaluation, and conclusions. Each step was built directly on the output of the preceding one, ensuring that the resulting artefact was both grounded in the existing body of knowledge and responsive to the needs identified in the SME cybersecurity awareness governance context. To establish a baseline for the identification and characterisation of the challenges currently faced by SMEs in CSA governance, the initial phase of the research consisted of a literature review (LR). This review mapped the current state of the field, synthesised existing findings, and highlighted the specific gaps that the subsequent phases of the research sought to address.

To maintain a consistent scope and ensure accessibility to an international audience, the review was restricted to literature published in English. Given the volume of available research and the pace at which the field evolves, this research began with a literature review covering the period from 2020 onwards and sought information using the following keywords: cybersecurity awareness, governance frameworks, SMEs, cybersecurity governance, cybersecurity framework, and the intersections among these concepts. The databases consulted during the LR phase included ScienceDirect, IEEE Xplore, Web of Science, Scopus, ProQuest, and Google Scholar. The search combined the keywords in different combinations, for example, by linking cybersecurity awareness with SMEs, governance, governance frameworks and cybersecurity frameworks. Sources were included when they addressed at least one of the following problems: CSA in SMEs, cybersecurity governance, board-level or management-level cybersecurity responsibility, SME-oriented cybersecurity frameworks, security awareness training or measurement of awareness and behaviour. Sources were excluded when they were outside the cybersecurity-awareness or governance scope, focused only on highly technical controls without organisational or governance relevance, addressed only large enterprises without transferable implications for SMEs, or did not provide sufficient relevance after abstract and content screening.

Alongside these academic databases, AI tools were used to supplement the manual search, surfacing relevant literature that the keyword-based approach had missed and locating important passages within the collected papers. The AI-supported search was used only as a supplementary aid: candidate sources and passages were manually checked before retention, and the paper's argumentation was based on the reviewed sources rather than AI-generated summaries. In addition, practitioner websites offering CSA services to SMEs were consulted to contextualise whether concerns similar to those identified in the academic literature were also visible in practice. These practitioner sources were used to contextualise the problem and identify recurring practical concerns, not as a substitute for the academic literature.

The Governance and operational barriers section presented earlier is the main synthesis output of this literature review: rather than serving as a generic introduction to the topic, it synthesises the findings extracted from the reviewed sources and presents the consolidated state of the art on CSA governance in SMEs. The recurring obstacles and gaps identified there served as the evidence base for

the subsequent DSR phases. The findings were grouped thematically into recurrent barriers, including governance-level awareness gaps, operational barriers, accountability issues, communication problems between IT and boards, and the gap between awareness and secure behaviour. These themes were then translated into design requirements for the proposed framework.

3.1. Design Science Research Process

As outlined above, the DSR process [41] structured the work into five iterative phases, each covering a specific role in the research process. Figure 1 summarises how the five DSR phases were operationalised in this study; each phase is described in more detail below.

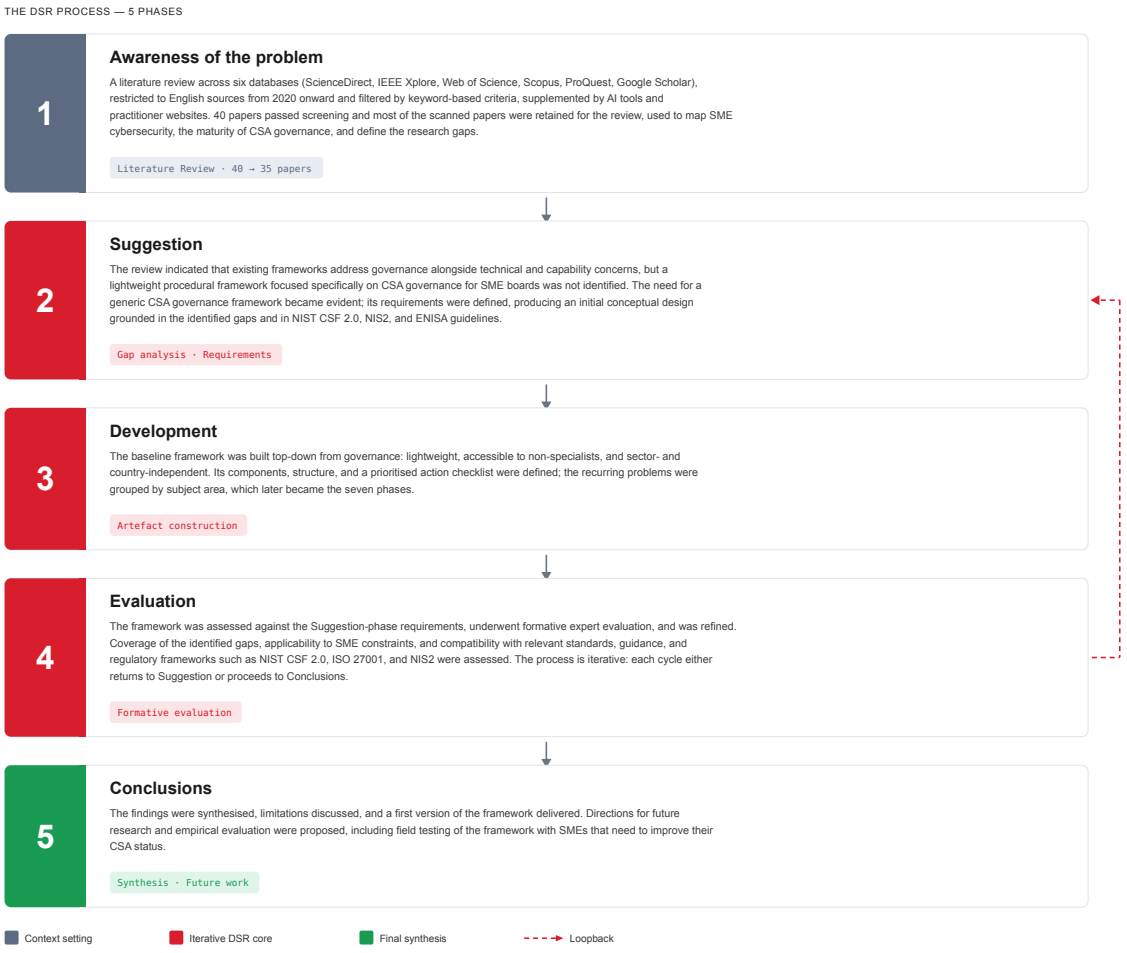


Figure 1: Overview of how DSR was employed in practice

Awareness of the problem: In this phase, the relevant publications were identified and inclusion and exclusion criteria were applied according to the scope, language, date and relevance criteria described above. After screening, 40 publications remained, of which 35 were retained as relevant to the study's scope. Five publications were excluded after relevance assessment because they did not sufficiently address the study's CSA-governance scope. This phase identified the current state of cybersecurity in SMEs and the maturity of CSA governance, mapped the existing frameworks, and defined the gaps that the research needed to address. The gaps identified in the literature were noted and regrouped by recurrence, relevance, and the type of problem they represented, along with potential solutions tailored to each problem. These gaps consisted of a set of obstacles that prevented SMEs from implementing effective cybersecurity measures. The governance gap, together with the recurring weaknesses of SMEs

and the need for more innovative training approaches, was further supported by the practitioner sources consulted, which reflected the same shortcomings observed in the academic literature. These obstacles extend beyond the commonly cited constraints and point to deeper structural and cognitive gaps at the governance level. These findings clustered into two distinct groups, reinforcing the argument that awareness must be governed, strategically directed, measured, and adapted rather than merely delivered:

The first group comprised operational barriers showing that, even when companies are willing to invest in cybersecurity, they struggle to translate that intention into action because there is no clear path to follow. These organisations often lack the resources, expertise, or clear guidance needed to translate that intention into action [3, 12]. The second group comprised governance-awareness gaps, whereby board members often lack sufficient knowledge of cybersecurity and its organisational importance. Consequently, they do not recognise the main reasons for investing in cybersecurity measures [28, 8].

Suggestion: The analysed literature showed that existing cybersecurity frameworks cover a broad range of technical, capability, risk-management, and governance concerns, but a dedicated procedural approach to CSA governance for SME boards remained underdeveloped. Substantial literature addressed specific cybersecurity problems, as well as some frameworks tailored for SMEs, but many were country- or sector-specific. The existing sector- and country-specific frameworks provided an important baseline from which the project began; they also contributed to the idea of linking most parts of the artefact to existing research and frameworks that might otherwise be difficult for non-specialists to identify and use. Several established standards and frameworks can nevertheless be demanding for resource-constrained SMEs to operationalise because of their breadth, implementation requirements, and need for specialised expertise [3, 12]. The resulting design opportunity was therefore to develop an accessible, sector-independent governance process focused specifically on CSA and intended for use by SME decision-makers. This need enabled the identification and definition of the framework requirements, producing an initial conceptual design grounded in the identified gaps and informed by existing models such as NIST CSF 2.0, NIS2, and ENISA guidelines.

Development: In this phase, the conceptual design produced during the Suggestion phase was turned into the framework baseline. It was constructed using a top-down approach that began with governance, with the goal of being lightweight, accessible to non-specialists, and adaptable across jurisdictions. Relevant elements from the models and frameworks retained during the Suggestion phase were identified and incorporated into the corresponding framework phases. This way, the artefact's components remained grounded in the existing models and frameworks. This stage defined the framework's components, structure, and sequence of actions that SMEs can follow to establish a baseline governance posture and a sequence of actions, together with the loopbacks that allow the process to be repeated as the company and its threat landscape evolve. A first draft was produced that grouped recurring problems by subject area, which later became the seven phases of the framework. To strengthen traceability, each phase was connected to the literature-derived problem it was intended to address and to the models or standards that informed it.

Evaluation: The framework was then assessed against the requirements defined in the Suggestion phase, reviewed by experts, and refined. This involved reviewing its coverage of the identified gaps, its applicability to SME constraints, and its compatibility with widely used regulatory requirements and standards, such as NIST CSF 2.0, NIS2, ISO 27001, and ENISA guidelines. Subsequently, several experts reviewed, evaluated and provided feedback on the artefact. The expert review focused on clarity, practical applicability for SME decision-makers, internal coherence between the phases, overlap between framework components and the explicit connection between the framework and the literature findings. The evaluation process was iterative: once the assessment was completed and feedback collected, the next step was either to return to the Suggestion phase or to move to the Conclusion phase to finalise the framework.

Conclusions: The feedback from the first iteration of the framework was discussed, and directions for future work and empirical evaluation were proposed. After the second iteration, the limitations identified are not seen as endpoints but are carried forward as inputs to the next design cycle, namely the planned field testing of the framework with SMEs that need to improve their CSA status. Since the

framework has not yet been empirically tested in live SME settings, the evaluation should be understood as a preliminary design evaluation rather than as evidence of practical effectiveness.

3.2. Artefact Development, Evaluation, and Refinement

At this stage, the framework had undergone two iterations. During the first iteration, the core content of each framework phase was developed. The issues identified during the research were listed and grouped by subject area, leading to an initial set of phases. The content of these phases was then refined, overlaps were removed, components were refined and extended, and connections to existing frameworks were made explicit.

The first version was evaluated in two ways. First, university professors provided expert feedback. Second, the framework was benchmarked against the regulatory and governance baselines with which it needed to remain compatible, including NIST CSF 2.0, NIS2, and ENISA guidance. Related models and frameworks were also considered, including CyberESP (An Integrated Cybersecurity Framework for SMEs) [42], ASMAS (Adaptable Security Maturity Assessment and Standardization) [43], and the conceptual cybersecurity governance model proposed by Yusif et al. [2]. This benchmarking indicated that the artefact focused more narrowly on the procedural governance of CSA while remaining broadly compatible with the wider governance, risk-management, and cybersecurity objectives of the compared frameworks. It was also consistent with the broader finding that no general cybersecurity governance framework has yet been established [37].

The evaluation helped sharpen the focus of the framework. The evaluation identified repetitions between phases, recommended the use of bullet points to improve accessibility, suggested a more specific focus for each phase, and asked that the connections between the framework and the research findings be made explicit. Based on this feedback, the phases were consolidated into seven, each with a distinct purpose. The activities within the phases were added, removed, moved, or reformulated to reduce overlap and improve the overall sequence.

Following the first review round, the revised framework was evaluated by one additional expert. This review emphasised the need to introduce each framework phase, explain its purpose, motivate the listed activities, and clarify its connection to the study's findings. In response, an introduction was added to each phase, and the tasks listed in the bullet points were linked more explicitly to the publications that informed them. References to relevant frameworks, standards, regulations, and empirical studies were also added within the phases themselves. For example, NIS2 and NIST CSF 2.0 were referenced in the phase addressing regulatory obligations.

The second review did not require major structural changes, but it led to further clarification of the phase descriptions and stronger traceability between the identified barriers, the selected design foundations, and the final framework phases.

3.3. Design Foundations

This section presents the theoretical models and governance concepts selected as design foundations for the proposed framework. Each component was chosen because it addresses one or more of the recurring governance or operational barriers identified in the LR. Together, these components provide the conceptual basis for the framework phases presented in Section 4.

The frameworks and models presented in this section were identified and selected because each addresses a distinct and recurrent gap in the literature, whether related to board-level decision-making, accountability structures, measurement of training effectiveness, or maturity tracking. Together, they form the building blocks of the CSA governance framework proposed in the following section. They are reported here individually, along with the specific problem each one addresses, to explain the rationale behind the framework's design and how its components were intended to work together when applied in practice.

3.3.1. Agency Theory and Cybersecurity Governance

Burch et al. [44] interpret NIST CSF 2.0 from an agency-theory perspective, emphasising that cybersecurity governance should take into account actors' responsibilities, incentives, and potential conflicts of interest. This perspective is relevant to the proposed framework because it frames CSA governance as a problem of accountability and alignment among organisational actors.

3.3.2. Critical Infrastructure Cyber Governance Maturity Model (CICGM)

The CICGM tool allows organisations to track progress across levels (e.g., S0 to S4), ensuring that awareness can be prioritised in the strategic plan. To provide a holistic view of an organisation's maturity, the model measures governance through three concurrent dimensions: governance level, cybersecurity functions, and governance components. By translating complex governance concepts into easy-to-understand, non-technical indicators, the model enables managers in resource-constrained environments to track progress and build a more competent workforce [45]. Although CICGM was developed for a critical-infrastructure context, its non-technical maturity structure is used in the proposed framework as a supporting approach for maturity assessment and progress tracking rather than as a prescriptive SME maturity standard.

3.3.3. Five lines of accountability model

Due to confusion over roles and responsibilities, employees often do not know whom to report an event to, particularly during emergencies, when quick, clear communication is needed. This model addresses this problem by clearly separating roles across the organisation and its levels. For the purposes of the proposed framework, the Five Lines of Accountability model [46] is operationalised as a chain spanning operational/frontline functions, risk-management functions, internal audit, executive management, and the board, thereby extending the traditional Three Lines model. This model ensures that responsibility roles are clear and well-defined, supporting smoother coordination, especially in the case of a cybersecurity incident, while reducing ambiguity in shared responsibilities [1, 46].

3.3.4. Importance of modern CSA employee training

Traditional CSA programmes have often relied on generic and relatively passive forms of instruction. More recent approaches emphasise contextual and interactive training, including game-based methods, to make security awareness activities more relevant to employees' actual work situations [25]. In addition, the effectiveness of CSA training should be assessed beyond participation or completion rates by considering changes in knowledge, attitudes, and behaviour [7]. These findings motivate the use of contextual, interactive, and measurable training activities in Phase 6 of the proposed framework.

3.3.5. CARE framework

Modi et al. [10] discuss the CARE framework as an approach for structuring security information into dimensions that can support board-level decision-making. It categorised security information into four digestible dimensions:

- **Consistency:** The reliability of security controls across the organisation.
- **Adequacy:** Whether the security programme meets the identified business needs.
- **Reasonableness:** The balance between security spending and actual risk reduction.
- **Effectiveness:** The measurable success of security resources in mitigating threats.

These dimensions were relevant for the proposed framework because they translate cybersecurity performance into categories that can support governance-level decision-making.

3.3.6. KAB model

The Knowledge, Attitude, and Behaviour (KAB) model [7] supports evaluating CSA beyond training completion or knowledge-test scores by distinguishing changes in knowledge, attitudes, and behaviour. Behavioural indicators may include performance in simulated phishing exercises or security-reporting behaviour. Within the proposed framework, KAB is therefore used to link awareness activities to measurable outcomes at different levels.

3.3.7. Board-Level Cybersecurity Governance

Gale et al. [8] conducted a study on cybersecurity from the perspective of BoDs. The study examined how cybersecurity is handled within companies, how it is communicated, and the strongest drivers of development. The findings showed that the biggest drivers for SMEs to invest in cybersecurity were normative compliance and being a victim of a cyberattack, that is, obligations and past experience. Any other kind of motivation not tied to concrete cases remained weak. During their interviews, it emerged that BoDs either avoided cybersecurity topics due to their lack of knowledge and awareness, or placed all the work on specific members whom they considered knowledgeable. In many cases, responsibility then shifted to the IT department, the CIO, and the CISO, who were burdened with this duty. Conversely, the IT personnel reported difficulty communicating reports clearly to the BoDs because no joint report format had been defined. A persistent failure in corporate environments was that board conversations about security often stopped at operational updates rather than focusing on actual governance. Taken together, these findings suggest that economic and regulatory considerations can provide useful entry points for engaging boards with cybersecurity, before more detailed technical risks and their business consequences are addressed.

These findings constituted one of the main empirical foundations informing the CSA governance framework.

Building blocks brought into the framework design

Building block	Source	Contribution / gap addressed	Phase
Major standards (NIST CSF 2.0, ISO 27001, NIS2, ENISA)	NIST CSF 2.0; ISO 27001; NIS2; ENISA guidance	Provide governance, regulatory, and capability reference points that may be demanding for resource-constrained SMEs to operationalise, motivating a lightweight CSA-focused layer.	Phase 2
Agency theory perspective	Burch (2024)	Frames cybersecurity governance as aligning incentives among organisational actors and anticipating conflicts of interest.	Phase 3
CICGM maturity model	Zwarts (2025)	Non-technical maturity scale (S0–S4) across governance level, functions and components that resource-constrained managers can track.	Phase 4
Five Lines of Accountability model	Slapnicar (2023)	Clear responsibility chain — frontline/IT, risk management, internal audit, executive management, board — removing role ambiguity during incidents.	Phase 5
Modern CSA training (role-tailored, interactive)	Chaudhary et al. [3, 8]; Kävrestad et al. [21]	Supports contextual, interactive, and role-relevant training, with effectiveness assessed beyond completion rates.	Phase 6
CARE framework	Modi et al. [11]	Board-readable security metrics in four dimensions: Consistency, Adequacy, Reasonableness, Effectiveness.	Phase 6
KAB model	Chaudhary (2022)	Measures training success through Knowledge, Attitude and Behaviour and behavioural indicators instead of completion tests.	Phase 6
Gale et al. board-level findings	Gale et al. (2022)	Drives separate assessment of governance awareness and jointly defined IT–board reporting standards; economic/legal framing as entry point.	Phases 3 & 5

Figure 2: The building blocks of the framework

4. The CSA Governance Framework

The common root of the governance problems identified in the literature is the lack of cybersecurity awareness at the board level, together with the absence of practical governance guidance for SMEs. Existing frameworks provide substantial support for cybersecurity governance and risk management, but the literature reviewed here indicates a need for a simpler procedural entry point focused specifically on how SME boards govern CSA [47]. To address this, the framework was built on the findings from the reviewed literature as a starting point, and these were structured into an iterative CSA governance process for board members to follow.

Its design was shaped by the two types of barriers identified in the DSR problem-awareness phase. The gaps in governance awareness, such as the lack of board-level cybersecurity knowledge [28, 8], the underestimation of exposure [12], and the lack of strategic motivation [36], require phases that establish a foundational understanding before taking action. The operational barriers, like the failure to include CSA in the business plan [11], the disconnect between IT reporting and board understanding [8], the gap between awareness and behaviour [5], require phases that turn governance awareness into organisational structures, measurable training, and ongoing improvement. This distinction shaped the overall structure, with each component addressing a specific problem: the early phases covered the governance awareness gap that must be resolved first, while the later phases addressed the operational barriers. The models mentioned in the framework are used as design foundations, needed to structure and support the framework. Intended users can follow the framework's seven phases as a structured process and consult the underlying models or standards when additional detail is required.

The seven phases were organised into three functional groups. Each serves a specific purpose within the CSA assessment process and provides the basis for the subsequent phases. Each design foundation identified during the Suggestion phase was incorporated into the framework phase that addresses the corresponding governance barrier. The first group, context setting, comprises Phases 1 and 2 and establishes the basis for the subsequent phases. These phases establish the organisational and regulatory context needed for the subsequent board-level assessment and should therefore be completed before Phase 3. The second group, governance and training, includes Phases 3-6. These phases begin with an assessment of board-level awareness and then move to accountability structures and measurable training. Phase 7 closes the cycle by establishing continuous monitoring and improvement.

The governance-focused core of the framework begins in Phase 3, where the board assesses its own CSA and accountability. This phase is informed by the agency-theory perspective discussed by Burch et al. [44], which highlights responsibilities, incentives, and potential misalignment among organisational actors. The findings from Gale et al. [8] on board-level communication failures influenced both Phase 3 and Phase 5 by requiring separate assessments of governance awareness and jointly defined reporting standards. The CICGM maturity model [45] was included in Phase 4 to offer a non-technical maturity scale (S0-S4) that resource-constrained managers can use. The five lines of accountability model [46] was integrated into Phase 5 to clarify the full responsibility chain from frontline staff to the board. This addresses the role ambiguity identified in the literature as a barrier to effective incident response. The KAB model [7] was added to Phase 6 to measure training outcomes using behavioural indicators instead of completion metrics. The CARE framework [10] was incorporated alongside it to provide the BoD with metrics structured into four dimensions (Consistency, Adequacy, Reasonableness, Effectiveness), to support interpretation of cybersecurity performance by non-technical board members.

Since the process is meant to be repeated during both the first assessment and periodic reviews, three loopbacks were built in. The first, from Phase 2 back to Phase 1, occurs when identifying the applicable regulations reveals that the company's sector or profile differs from the initial assumption. The second, from Phase 5 back to Phase 3, occurs when defining the roles exposes governance gaps at the board level that call for reassessment of board-level awareness and accountability. The third, from Phase 7 back to Phase 1, restarts the whole process whenever continuous monitoring detects a change in the threat landscape or in the business model.

4.1. Framework Phases

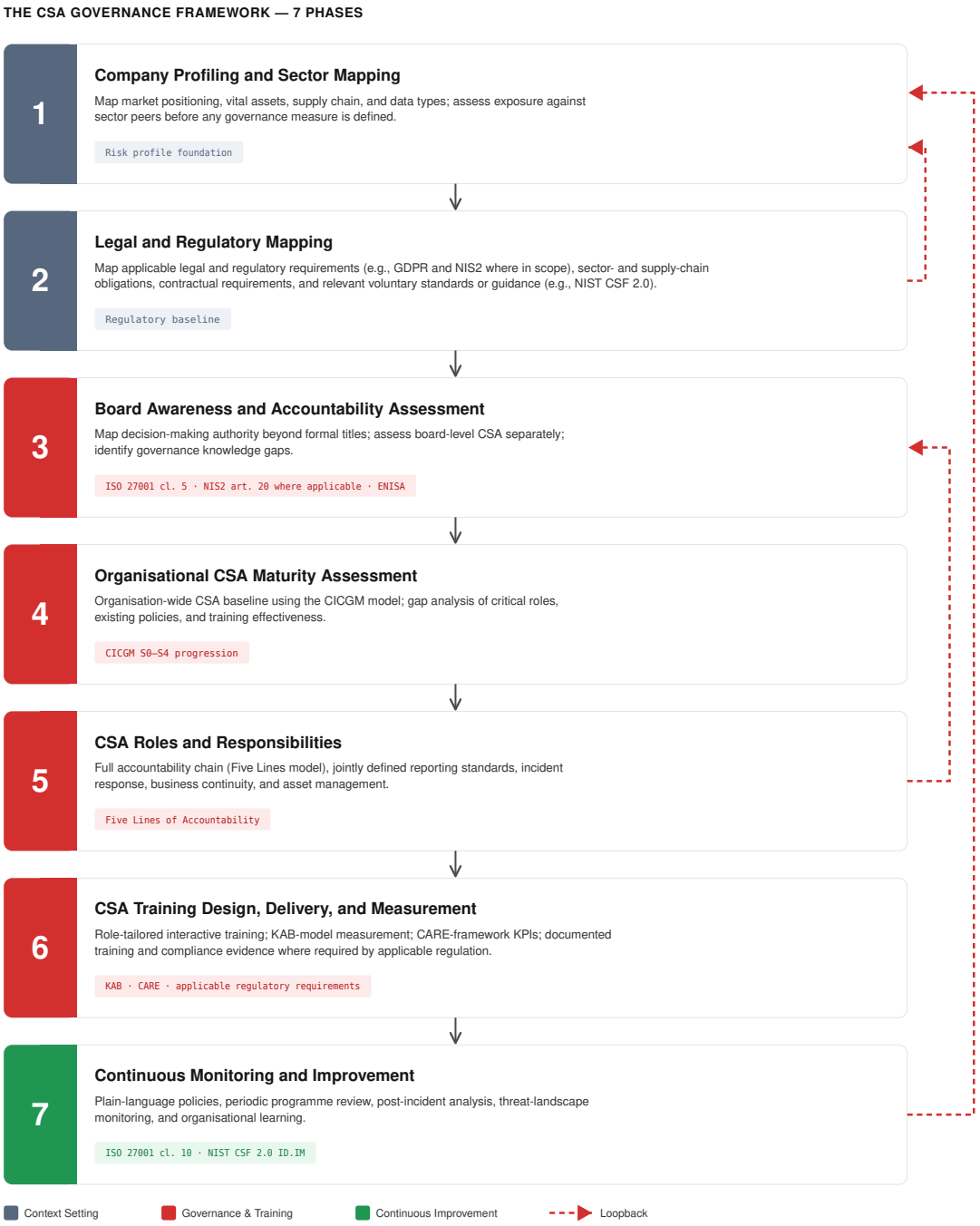


Figure 3: Scheme of the CSA governance framework

Phase 1: Company Profiling and Sector Mapping

This is the discovery phase, during which information about the company is gathered and verified. Establishing an accurate picture of the company context is important because it provides the basis for the subsequent phases. The literature reports that SME decision-makers may underestimate cyber risks [11, 12], highlighting the value of systematically making the organisation's risk context visible at the governance level [19]. This phase requires decision-makers to map their market position, data assets, supply chain dependencies, and sector-specific risk factors before defining governance measures. The

tasks draw on the contextual profiling approach described by Chang et al. [36] and on the finding that the failure to integrate CSA into the business plan is one of the most recurrent governance barriers [11, 35].

- Review existing risk-analysis documentation and identify gaps or areas requiring update.
- Document the company's size, market context, critical assets, supply-chain dependencies, and operating jurisdictions [36].
- Record the jurisdictions, sectors, and supply-chain relationships that may trigger specific legal, regulatory, or contractual requirements; detailed mapping of these requirements is undertaken in Phase 2.
- Assess the company's level of exposure and compare it with similar companies in the same sector.
- Map the types of data processed and the critical digital assets the business depends on. This will determine the company's risk profile and set the direction for the following phases.

Phase 2: Legal and Regulatory Mapping

Once the company's context and risk profile are clear, the next step is to determine which laws and requirements apply and must be followed. Gale et al. [8] found that regulatory obligations and the threat of penalties are the strongest drivers of board engagement with cybersecurity. Yet, boards still frequently lack awareness of which regulations apply to them. This phase requires a systematic mapping of the laws and regulations applicable to the organisation, together with relevant sector-specific, contractual, and supply-chain obligations. Voluntary standards and guidance, such as NIST CSF 2.0 [15], may then be mapped separately to support implementation. In the EU, relevant legislation may include GDPR [48] and, for organisations within its scope, NIS2 [16]; other requirements will depend on the organisation's sector, activities, and jurisdiction. A loopback to Phase 1 is built into this stage, as newly identified regulatory requirements may alter the company's risk profile or sector classification.

- Verify mandatory legal and regulatory requirements in the jurisdictions in which the company operates, as well as other standards or contractual requirements based on the sector in which the company operates.
- Analyse regulatory requirements, ensuring that the awareness programme satisfies existing legal and regulatory obligations.
- Identify any sector-specific and supply-chain regulatory requirements or compliance expectations that add to the baseline. Failure to meet applicable requirements may expose the organisation to legal, regulatory, contractual, or commercial consequences.
- Cyber-insurance providers may also impose cybersecurity prerequisites or conditions of coverage, which should be identified where relevant.

Phase 3: Board Awareness and Accountability Assessment

The goal of this phase is to assess the board's cybersecurity awareness and establish accountability at the board level before any organisation-wide role structure is defined. Where internal expertise is insufficient, external cybersecurity expertise may be used to support the assessment. The literature documents that board members either avoid cybersecurity topics due to their lack of knowledge, or delegate all responsibilities to a single individual perceived to have the requisite expertise, typically the CISO or an IT manager [8]. This phase aims to avoid such concentration of responsibility by establishing shared board-level understanding and explicit accountability rather than concentrating cybersecurity responsibility in a single individual, while the full organisation-wide chain of roles and responsibilities is defined later in Phase 5.

- Where needed, obtain appropriate external cybersecurity expertise.
- Identify all individuals who hold strategic decision-making authority, regardless of their formal titles. An agency-theory perspective highlights that decision-making authority may not align with formal titles [44]. In SMEs, strategic decision-making authority may extend beyond formal job titles and formally assigned responsibilities.

- Identify board-level responsibilities instead of treating cybersecurity as only an IT role, and establish a baseline for reporting procedures. This is consistent with the leadership and governance principles in ISO 27001 Clause 5 [14] and, for entities within its scope, the management-body responsibilities established in NIS2 Article 20 [16].
- Verify that the board has oversight of how CSA training is assigned, completed, evaluated, and improved, rather than monitoring completion alone.
- Assess the board's CSA level separately from the rest of the organisation, since board members need a different kind of training compared to other employees [36].
- Identify specific knowledge gaps before proceeding to the following phase.

Phase 4: Organisational CSA Maturity Assessment

This phase assesses the company's current CSA status and the organisation's existing CSA practices and measures. Where prior CSA training exists, its results are reviewed to identify gaps and inform the design of the future training programme. Based on these results, the analysis of the situation, and the outcomes of the previous phase, the areas that need more attention are identified. This will be necessary to focus the future planning phase and allocate limited resources effectively. The CICGM model [45] is used here as an optional reference for structuring maturity assessment and identifying areas for improvement.

- Conduct a CSA baseline assessment to understand the overall organisational awareness level.
- Understand the cybersecurity posture of the company and what measures have already been put in place.
- Identify the most critical assets and roles that are most exposed to potential attacks.
- Where appropriate, tools such as CyberESP [42] may support parts of the asset-identification and assessment process and reduce reliance on fully manual analysis.
- Identify priority gaps and document remediation actions with target completion dates.
- Document current training activities, policies, and their effectiveness in order to produce a gap analysis that will shape the future training programme design.
- Where appropriate, use the CICGM model to characterise the current CSA maturity level and identify improvement goals. This can be particularly useful for SMEs where size and budget constraints are critical [45]. Because CICGM is an emerging model and has not yet been extensively validated across SME contexts, it should be treated as a supporting assessment approach rather than as a definitive maturity standard.

Phase 5: CSA Roles and Responsibilities

This phase operationalises the governance awareness established in Phase 3 by defining the full accountability chain across the organisation. The five lines of accountability model from Slapnicar et al. [46] provides the structural backbone for this phase, extending the traditional three lines of accountability by adding executive management and the board as the fourth and fifth lines, respectively. Oh et al. [1] contribute to the governance value chain perspective, in which roles from the board down are clearly outlined through governance structures that ensure interdepartmental collaboration and coordination, with the CISO reporting to both the board and the risk committee. Gale et al. [8] highlight the need for reporting practices that support communication between IT personnel and the board, addressing a recurring source of communication difficulty. A loopback to Phase 3 is included, as defining roles may reveal previously hidden governance gaps.

- The board retains governance oversight and accountability for CSA, while operational responsibilities for training and cybersecurity activities may be delegated to management, IT/security functions, or external providers [1].
- Define the chain of awareness responsibility from the board to management to employees. The organisation can adapt the Five Lines of Accountability model [46] to its size and structure in order to establish a clear chain of responsibilities. Everyone must have a clear role; knowing what to do and whom to report to or contact is key to a quick response in the event of an incident or data breach.

- Establish reporting standards that both the BoD and IT can understand, and define regular intervals for presenting cybersecurity reports to the board.
- Define employees' awareness, reporting, and communication responsibilities within the organisation's existing incident-response and business-continuity arrangements.
- Check and update the asset list and its management procedures [8].
- Document the CSA programme through clear policies and procedures written in plain language so that employees can understand and apply them. The use of clear and specific policies is consistent with the governance and policy principles reflected in ISO 27001, NIS2 where applicable, and NIST CSF 2.0.

Phase 6: CSA Training Design, Delivery and Measurement

This phase translates the governance and organisational structures from the preceding phases into a concrete, organised training programme. It integrates the KAB model from Chaudhary et al. [7], which measures training outcomes through knowledge, attitude, and behavioural indicators, and the CARE framework from Modi et al. [10], which structures security metrics into four dimensions comprehensible to non-technical board members. Prior research supports contextual and interactive approaches to CSA training, including game-based methods [25], while evaluation frameworks emphasise measuring outcomes in terms of knowledge, attitudes, and behaviour rather than relying only on participation or completion metrics [7].

- Design a CSA training programme that addresses the needs identified in the preceding phases while remaining feasible within the organisation's available resources.
- Evaluate the effectiveness of the training programme and tailor activities to employees' roles, knowledge gaps, and risk exposure where appropriate.
- Use contextual and interactive training approaches where appropriate [25].
- Monitor and measure the training outcomes and effects by analysing their results using the KAB model instead of only relying on completion rates [7]. Major cybersecurity standards, frameworks, and guidance, including ISO 27001 [14], ENISA [17], and NIST [15], emphasise monitoring and continual improvement.
- Define indicators for evaluating training outcomes and tracking changes over time, using measures such as KAB outcomes, simulated-phishing detection and reporting rates, and other behavioural measures appropriate to the organisation [10, 7].
- Track employees' training completion and report the results to the board; this allows the organisation to monitor progress and adjust the programme to identified needs.
- Training activities should be documented where this is required by applicable legal, regulatory, contractual, or governance requirements. For example, NIS2 establishes training obligations for management bodies of entities within its scope, while GDPR Article 39 identifies awareness raising and training of staff involved in processing operations as part of the data protection officer's monitoring tasks.

Phase 7: Continuous Monitoring and Improvement

This final phase formalises the framework's iterative nature through a continuous review cycle. It is aligned with ISO 27001 Clause 10 [14] and the NIST CSF 2.0 Improvement category (ID.IM) [15], which emphasise continual improvement and learning from evaluation and operational experience. Hoong and Rezania [47] provide a rationale for treating adaptation as an integral part of cybersecurity governance rather than as a one-time activity. In the proposed framework, this principle is operationalised through periodic review of governance arrangements, training outcomes, incident lessons, and changes in the organisation's risk context. A loopback to Phase 1 ensures that changes in the threat landscape or business model trigger a complete reassessment.

- Review and update plain-language cybersecurity policies as part of the continuous improvement cycle so that they remain understandable, relevant, and aligned with current organisational practices [40].

- Policies should address key areas such as incident reporting, password and access management, data handling, use of organisational devices, and controls associated with critical assets.
- Review the CSA programme at planned intervals and whenever significant organisational, regulatory, incident-related, or threat-related changes occur.
- Where appropriate, conduct phishing simulations or reporting exercises to assess relevant aspects of employee detection and reporting behaviour and to identify areas requiring further training.
- After an incident, conduct a post-incident review to identify contributing factors, what worked, what failed, the consequences, and necessary improvements.
- Monitor changes in the organisation's threat, regulatory, and operational context and feed relevant lessons into subsequent governance, policy, and training decisions.

5. Discussion

A central recurring problem identified in the review is the absence of an accessible governance-level process that brings the different CSA-related barriers together. This interpretation is consistent with Mumford's [13] broader argument that complex technological problems require organisational approaches to decision-making rather than isolated technical responses. What is needed is a simple, accessible, yet sufficiently detailed framework that enables SMEs to work towards greater cybersecurity maturity and regulatory alignment. The framework provides a structured sequence of actions for establishing a baseline governance posture.

While NIST CSF and ENISA provide useful guidance for SMEs, frameworks such as CyberESP [42] and ASMAS [43] address complementary needs, including technical risk management and maturity assessment. The proposed framework instead focuses specifically on organising board-level CSA governance and is therefore intended to complement, rather than replace, these approaches.

The literature documents that IT departments struggle to present cybersecurity information in terms that are meaningful for governance decision-making, while boards lack the baseline knowledge required to interpret technical reports [8, 46]. By requiring boards to first establish their own baseline understanding in Phase 3 before defining reporting standards and accountability chains in Phase 5, the framework creates the conditions to reduce this communication gap and establish a clearer communication protocol.

The framework also responds to the finding that SME governance bodies are often reactive rather than proactive: the strongest drivers for board engagement remain normative compliance and having been the victim of an attack, while preventive motivators are comparatively weak [8]. To address this problem, the organisational risk context established in Phase 1 and the legal and regulatory obligations mapped in Phase 2 are intended to provide a stronger strategic basis for board engagement, addressing what the literature identifies as a lack of structured mechanisms to make the economic case for CSA [19, 8].

5.1. Limitations

This study has several limitations. Most importantly, the framework has not yet been evaluated empirically in a live SME environment. Although its phases are grounded in the reviewed literature and informed by established standards and frameworks, its practical effectiveness and utility remain to be demonstrated, including whether board members can understand and follow it independently, whether it produces measurable improvements in awareness, and whether it leads to downstream adoption of technical frameworks. The literature review was limited to recent English-language publications from 2020 onward, potentially excluding relevant findings published in other languages or earlier periods. The selection process relied on abstracts and keyword screening, which may have excluded papers with relevant content that was not reflected in their titles or abstracts; additionally, excluding five papers based on content-relevance judgments may have introduced selection bias. The review also includes preprints and practitioner sources (e.g. [11, 28, 24]). These sources were used selectively,

but their inclusion reduces the evidential strength of claims that are not independently supported by peer-reviewed or primary sources.

The framework assumes a minimum organisational structure, which may not hold for the smallest micro-enterprises, where the owner performs all functions. While the sector-agnostic design enables broad applicability, it lacks the depth required for industries with highly specific regulatory or threat environments such as healthcare, finance, or critical infrastructure, where additional layers would be needed. The regulatory references are cited as alignment points rather than detailed compliance mappings, since the framework is intended to be independent of the country of application. Organisations pursuing formal certifications will still require professional guidance beyond what the framework provides, since it is not intended for that purpose. Lastly, the evaluation phase of the DSR process was limited to a structural comparison against the requirements identified in the Suggestion phase and a limited number of expert reviews; it did not include in-depth practitioner feedback or field testing in SMEs.

5.2. Contributions

The CSA governance framework proposed in this paper is designed as a complementary governance layer that can support SMEs in making effective use of broader technical, risk-management, and maturity-oriented frameworks, and makes several contributions to the field. In terms of academic contribution, two main contributions can be noted:

First, it proposes and operationalises a definition of CSA governance for the SME context, addressing an area that remains comparatively underdeveloped in the literature. Across this paper, CSA governance has been defined as the set of responsibilities and practices through which an SME board and executive management provide strategic direction for CSA. Rather than focusing primarily on operational or technical controls, the proposed construct focuses specifically on the governance processes through which SME boards establish direction, accountability, and oversight for CSA. It is inherently procedural, unfolding as a structured sequence that moves from understanding the organisation's risk profile, and through establishing accountability structures and mapping applicable regulatory obligations, to designing, sustaining, measuring, and continuously improving a CSA programme. Its defining principle is that awareness should be governed rather than merely delivered, as clear governance structures and board-level oversight can support the continuity and effectiveness of CSA activities and related controls. By operationalising this sequence, the framework builds upon classic socio-technical system design paradigms, such as Mumford's ETHICS approach [29], which similarly emphasises the need to consider organisational and human factors alongside technical system design.

Second, the framework synthesises several established models, including the Five Lines of Accountability [46], the CARE and KAB measurement models [7, 10] and the emerging CICGM maturity model [45] into a single governance process. These models originate in different strands of the literature; the proposed framework brings selected elements together within a single governance process.

The framework also makes two practical contributions:
First, by targeting the governance layer specifically, this framework is positioned in a space that existing technical and maturity frameworks do not fully address: it does not replace the main existing frameworks but rather provides governance-level preparation that may support the later adoption of those tools.
Second, the loopback cycles provide an explicit mechanism for organisational learning and continuous review within the proposed governance process.

5.3. Future research

Several directions for future work can follow from this first version of the framework. The most immediate next step is to evaluate the framework with SMEs across different sectors and sizes to assess whether board members can follow the phases independently, and whether the framework produces measurable improvements in governance-level awareness and downstream security behaviour.

Replicating and extending the qualitative approach used by Gale et al. [8] by interviewing board members before and after framework adoption would provide valuable insight into whether plain-language and business-oriented framing effectively motivates governance engagement and how such framing is perceived by SME decision-makers.

A structured expert review involving cybersecurity consultants, auditors, and governance professionals would help refine the phase structures and identify practical gaps that the literature alone cannot reveal.

A detailed mapping between each framework phase and relevant NIS2 provisions, ISO 27001 clauses, and NIST CSF 2.0 outcomes could improve regulatory and standards traceability and increase its value for SMEs seeking regulatory alignment, formal assurance, or relevant certification.

Finally, the development of a lightweight digital self-assessment tool would allow SMEs to track their progress through the seven phases, measure improvements over time, and generate board-ready reports. This tool would significantly increase practical adoption and provide the quantitative data needed to evaluate the framework at scale.

6. Conclusions

Well-established standards and frameworks provide substantial support for cybersecurity governance and risk management, including governance-oriented guidance. The more specific gap addressed in this paper concerns an accessible procedural approach for governing CSA at board level in resource-constrained SMEs. Further research on CSA governance is needed, particularly regarding SME board needs and the practical effects of governance-oriented interventions.

The DSR methodology [41] provided the structure for moving from the literature-derived problem analysis to the design, formative evaluation, and refinement of the seven-phase framework. Two design iterations were used to reduce overlap between phases, strengthen their connection to the literature, and clarify the framework for its intended users.

This paper contributes a structured conceptualisation of CSA governance and a seven-phase process intended to help SME boards translate awareness of cybersecurity risks and responsibilities into organisational action. This conceptualisation of CSA governance helps articulate the relationship between cybersecurity awareness activities and broader organisational cybersecurity governance. By providing a practical, step-by-step guide for SMEs, the framework is designed to be simple enough for non-expert decision-makers to apply its recommendations. A key feature is the explicit linkage to underlying models and standards, which users can consult when additional detail is required. In this way, the user is guided to other frameworks that address specific needs, allowing the organisation to move towards its cybersecurity goals.

7. Declaration on Generative AI

During the preparation of this work, the authors used Grammarly, Claude Opus 4.8, Sonnet 5, and ChatGPT 5.5 to perform grammar and spelling checks, check for duplications, improve writing style, and generate the images. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

Acknowledgments

We gratefully acknowledge the financial support provided by the Knowledge Foundation (KKS) through the project *Cybersecurity Awareness in Production (CyProd)*, reference number 20250064.

References

[1] K. B. Oh, G. Hoang, J. Sturdy, S. S. Guo, Cybersecurity Governance: An Enterprise Risk Management Strategy for Cyber Risk Control, 1 ed., Springer Singapore, Singapore, 2025. doi:10.1007/978-981-95-3865-2.

[2] S. Yusif, A. Hafeez-Baig, A conceptual model for cybersecurity governance, Journal of Applied Security Research 16 (2021) 490–513. doi:10.1080/19361610.2021.1918995.

[3] S. Chaudhary, V. Gkioulos, S. Katsikas, A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises, Computer Science Review 50 (2023) 100592. doi:10.1016/j.cosrev.2023.100592.

[4] N. Khan, S. Furnell, M. Bada, M. Rand, J. R. C. Nurse, Investigating the experiences of providing cyber security support to small- and medium-sized enterprises, Computers & Security 154 (2025) 104448. doi:10.1016/j.cose.2025.104448.

[5] M. de Bruin, K. Mersinas, Individual and contextual variables of cyber security behaviour: An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour, CoRR abs/2405.16215 (2024). doi:10.48550/arXiv.2405.16215.

[6] Verizon Business, 2024 Data Breach Investigations Report, Technical Report, Verizon Business, 2024.

[7] S. Chaudhary, V. Gkioulos, S. Katsikas, Developing metrics to assess the effectiveness of cybersecurity awareness program, Journal of Cybersecurity 8 (2022) tyac006. doi:10.1093/cybsec/tyac006.

[8] M. Gale, I. Bongiovanni, S. Slapničar, Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead, Computers & Security 121 (2022) 102840. doi:10.1016/j.cose.2022.102840.

[9] J. J. Fay, D. Patterson, Contemporary Security Management, 4 ed., Butterworth-Heinemann, Oxford, UK, 2018. doi:10.1016/C2015-0-04732-3.

[10] A. Modi, I. Kuzminykh, B. Ghita, Data driven approaches to cybersecurity governance for board decision-making: A systematic review, CoRR abs/2311.17578 (2023). doi:10.48550/arXiv.2311.17578.

[11] C. Rombaldo Junior, I. Becker, S. Johnson, Unaware, unfunded and uneducated: A systematic review of SME cybersecurity, CoRR abs/2309.17186 (2023). doi:10.48550/arXiv.2309.17186.

[12] M. Kappe, R.-C. Härting, C. Karg, D. Deffner, Cybersecurity in SMEs: Drivers of cybercrime, insufficient equipment and prevention, Procedia Computer Science 225 (2023) 3631–3640. doi:10.1016/j.procs.2023.10.358.

[13] E. Mumford, Dangerous Decisions: Problem Solving in Tomorrow's World, 1 ed., Springer, New York, NY, 1999. doi:10.1007/b102291.

[14] International Organization for Standardization, ISO/IEC 27001:2022 information security, cybersecurity and privacy protection — information security management systems — requirements, International Standard, 3rd ed., 2022.

[15] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, Technical Report NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, 2024. doi:10.6028/NIST.CSWP.29.

[16] European Parliament and Council of the European Union, 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 (NIS 2 Directive), 2022. Official Journal of the European Union, L 333, pp. 80–152, 27 December 2022.

[17] European Union Agency for Cybersecurity (ENISA), Cybersecurity Guide for SMEs: 12 Steps to Securing Your Business, Technical Report, European Union Agency for Cybersecurity (ENISA), 2021.

[18] G. Erdogan, R. Halvorsrud, C. Boletsis, S. Tverdal, J. B. Pickering, Cybersecurity awareness and capacities of SMEs, in: Proceedings of the 9th International Conference on Information Systems Security and Privacy, INSTICC, SciTePress, 2023, pp. 296–304. doi:10.5220/0011609600003405.

[19] Y. Hoong, D. Rezania, R. Baker, When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands, Technology in Society 78 (2024) 102650. doi:10.1016/j.techsoc.2024.102650.

[20] European Commission, Commission recommendation of 6 may 2003 concerning the definition of micro, small and medium-sized enterprises (2003/361/EC), 2003. Official Journal of the European Union, L 124, pp. 36–41, 20 May 2003.

[21] A. Alexei, A. Alexei, The problem of information systems security in SME, in: Proceedings of the Central and Eastern European eDem and eGov Days 2023, ACM, Budapest, Hungary, 2023, pp. 101–105. doi:10.1145/3603304.3603346.

[22] T. Luor, J. F. Wang, Bridging the gap between cybersecurity awareness and implementation: A three-stage healthcare metaphor for cross-sector governance, International Journal of Information Security 25 (2026) 18. doi:10.1007/s10207-025-01186-x.

[23] R. West, S. Michie, A brief introduction to the COM-B model of behaviour and the PRIME theory of motivation, Qeios (2021). doi:10.32388/WW04E6.3.

[24] H. Naaz, A. Faisal, Cybersecurity for SMEs: Innovative training solutions to address human error and strengthen security, ResearchGate preprint, 2024. doi:10.13140/RG.2.2.17143.53921.

[25] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, S. Furnell, Evaluation of contextual and game-based training for phishing detection, Future Internet 14 (2022) 104. doi:10.3390/fi14040104.

[26] M. Lennartsson, J. Kävrestad, M. Nohlberg, Exploring the meaning of usable security: A literature review, Information and Computer Security 29 (2021) 647–663. doi:10.1108/ICS-10-2020-0167.

[27] A. Clark, S. Mujeye, A critical analysis of SME cybersecurity policies and practices, in: Proceedings of the 2025 8th International Conference on Software Engineering and Information Management, ACM, 2025, pp. 178–183. doi:10.1145/3725899.3725926.

[28] O. Olabode, The relevance of cybersecurity awareness training for employees in small and medium enterprises (SMEs), ResearchGate manuscript, 2023. doi:10.13140/RG.2.2.21320.90883.

[29] E. Mumford, Effective Systems Design and Requirements Analysis: The ETHICS Approach, Information Systems Series, 1 ed., Macmillan, Basingstoke, UK, 1995. doi:10.1007/978-1-349-13774-9.

[30] K. Johansson, T. Paulsson, E. Bergström, U. Seigerroth, Improving cybersecurity awareness among SMEs in the manufacturing industry, in: A. H. C. Ng, et al. (Eds.), Proceedings of the 10th Swedish Production Symposium (SPS 2022), volume 31 of *Advances in Transdisciplinary Engineering*, IOS Press, 2022, pp. 209–216. doi:10.3233/ATDE220140.

[31] E. Bergström, J. Kävrestad, J. H. Gustafsson, H. Jonsson, Factors influencing the adoption of awareness-raising activities in SMEs, in: P. Bednar, J. Kävrestad, E. Bergström, M. Rajanen, H. Vallo Hult, A. M. Braccini, A. S. Islind, F. Zaghloul (Eds.), Proceedings of the 10th International Conference on Socio-Technical Perspectives in Information Systems (STPIS 2024), volume 3857 of *CEUR Workshop Proceedings*, CEUR-WS.org, 2024, pp. 118–131.

[32] F. Alharbi, M. Alsulami, A. Al-Solami, Y. Al-Otaibi, M. Al-Osimi, F. Al-Qanor, K. Al-Otaibi, The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in saudi arabia, Sensors 21 (2021) 6901. doi:10.3390/s21206901.

[33] A. Shojaifar, H. Järvinen, Classifying SMEs for approaching cybersecurity competence and awareness, in: Proceedings of the 16th International Conference on Availability, Reliability and Security, ACM, 2021, pp. 1–7. doi:10.1145/3465481.3469200.

[34] L. Gao, T. G. Calderon, Cybersecurity risk governance and companies' cybersecurity risk disclosures in their 10-k filings, Journal of Accounting and Public Policy 54 (2025) 107376. doi:10.1016/j.jaccpubpol.2025.107376.

[35] A. Chidukwani, S. Zander, P. Koutsakis, A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations, IEEE Access 10 (2022) 85701–85719. doi:10.1109/ACCESS.2022.3197899.

[36] Y. Chang, O. Heller, Y. Shlomo, I. Bar-Noy, E. Bokobza, M. Grinstein-Weiss, N. Zhang, Mind the gap: Revealing security barriers through situational awareness of small and medium business key

decision-makers, CoRR abs/2506.10025 (2025). doi:10.48550/arXiv.2506.10025.
[37] S. Savaş, S. Karataş, Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance, International Cybersecurity Law Review 3 (2022) 7–34. doi:10.1365/s43439-021-00045-4.
[38] A. Aleem, A. Wakefield, M. Button, Addressing the weakest link: Implementing converged security, Security Journal 26 (2013) 236–248. doi:10.1057/sj.2013.14.
[39] O. Cox, H. Kanji, Building effective cybersecurity governance, Harvard Law School Forum on Corporate Governance, 2022.
[40] M. Sadok, S. Alter, P. M. Bednar, It is not my job: Exploring the disconnect between corporate security policies and actual security practices in SMEs, Information and Computer Security 28 (2020) 467–483. doi:10.1108/ICS-01-2019-0010.
[41] V. K. Vaishnavi, W. Kuechler, Design Science Research Methods and Patterns: Innovating Information and Communication Technology, 2 ed., CRC Press, Boca Raton, FL, 2015. doi:10.1201/b18448.
[42] J. A. Calvo-Manzano, T. San Feliu, Á. Herranz, J. Mariño, L.-Å. Fredlund, A. M. Moreno, CyberESP: An integrated cybersecurity framework for SMEs, Journal of Software: Evolution and Process 37 (2025) e70050. doi:10.1002/smr.70050.
[43] B. Y. Özkan, M. Spruit, Adaptable security maturity assessment and standardization for digital SMEs, Journal of Computer Information Systems 63 (2023) 965–987. doi:10.1080/08874417.2022.2119442.
[44] G. F. Burch, J. Burch, M. McGarry, Cybersecurity risk management governance: An agency theory perspective, ISACA Journal (2024).
[45] H. Zwarts, J. Du Toit, B. Von Solms, Augmenting cybersecurity awareness at critical infrastructures in developing countries through a cybersecurity governance maturity model, in: Proceedings of the 24th European Conference on Cyber Warfare and Security, volume 24, 2025, pp. 726–733. doi:10.34190/eccws.24.1.3708.
[46] S. Slapničar, M. Axelsen, I. Bongiovanni, D. Stockdale, A pathway model to five lines of accountability in cybersecurity governance, International Journal of Accounting Information Systems 51 (2023) 100642. doi:10.1016/j.accinf.2023.100642.
[47] Y. Hoong, D. Rezania, Navigating cybersecurity governance: The influence of opportunity structures in socio-technical transitions for small and medium enterprises, Computers & Security 142 (2024) 103852. doi:10.1016/j.cose.2024.103852.
[48] European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation), 2016. Official Journal of the European Union, L 119, pp. 1–88, 4 May 2016.