FMDB *Transactions on Sustainable Organisational Practices*

A PMO-Led Cybersecurity Integration Framework for Enhancing Governance in SMEs

Raja Poudel[1,*]

[1]Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne, England, United Kingdom.
raja2.-@northumbria.ac.uk[1]

Abstract: Over 99% of EU companies are SMEs, yet resource constraints, lack of cybersecurity professionals, and maturity prevent them from implementing adequate cybersecurity precautions. SME PMOs prioritise time, budget, and scope, leaving cybersecurity to IT or to be ignored. This research creates a PMO-led Cybersecurity Integration Framework for SMEs with 10 to 250 staff and modest IT resources to integrate cybersecurity governance into project management. The systematic study of 2019–2025 peer-reviewed papers is grounded in pragmatism and design science. Here are notable cyberattack case studies. SME resource gaps, lack of PMO domain integration, late-stage security integration in the Waterfall project development model, clashes between Agile speed and cybersecurity priorities, or inappropriate corporate frameworks for SME cybersecurity were noted in the literature review. Three recurrent project management difficulties, invisible risk, no security budget, and unclear security responsibility ownership were found in HSE Ireland ransomware attacks (€100M+ damage, four months' recovery) and MOVEit supply chain hack (2700+ enterprises, 93 million individuals The framework has twelve components in four functional groups: Waterfall Security Integration (FR-01–FR-05), Agile Security Integration (FR-06), Standing Security Projects (FR-07–FR-08), and PMO Governance. This system uses integration, risk-proportionate governance, forcing functions over optional checkpoints, continuous protection, and methodology-agnostic design. Counterfactual validation reveals the method would have solved governance weaknesses that caused breaches. The research presents theoretical foundations and practical templates for security-unsavvy SMEs.

Keywords: Project Management; Cybersecurity Integration Framework; Waterfall Project Development; Unclear Security; Agile Security Integration; Corporate Frameworks.

Received on: 15/06/2025, **Revised on:** 18/08/2025, **Accepted on:** 01/10/2025, **Published on:** 05/03/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSOP

DOI: https://doi.org/10.69888/FTSOP.2026.000614

Cite as: R. Poudel, "A PMO-Led Cybersecurity Integration Framework for Enhancing Governance in SMEs," *FMDB Transactions on Sustainable Organisational Practices*, vol. 1, no. 1, pp. 45–68, 2026.

1. Introduction

Small and medium-sized enterprises (SMEs) are the backbone of the global economy, accounting for more than 99% of all organizations operating in the European Union and making a substantial contribution to employment and GDP [18]. Given the rapid pace of digitalization, SMEs increasingly use information technology to facilitate their business operations, thereby facing

[*]Corresponding author.

emerging risks. However, SMEs continue to face many challenges in implementing effective cybersecurity practices. Unlike corporations, SMEs do not have a dedicated security team or a Chief Information Security Officer (CISO), with overall cybersecurity responsibilities handled by employees with other responsibilities [8]. Limited budgets for IT and cyber security to implement enterprise-class solutions are hindered by the time and expertise required to implement advanced cyber security practices [27]. There is a significant gap between project governance and cybersecurity needs in an SME context. Project Management Offices (PMOs), to the extent they are implemented, tend to focus primarily on the classical constraints of time, cost, and scope. In contrast, security is rarely, if at all, considered in project governance [35]. Instead, security is relegated to isolated silos of IT, whereas projects represent both risks and opportunities for including security from inception. The inspiration to undertake this research stems from professional practice in IT and project management, and ultimately from a desire to apply my expertise in cybersecurity project management [37]. From first-hand experience, the paper found that changes instituted through PMO processes yield significant organisational impact because the awareness generated by process-oriented objectives influences all employees who participate in project delivery. This perception drives my research choice: PMO-managed approaches to cybersecurity integration will lead to much safer project management practices.

1.1. Problem Statement

SMEs face a fundamental challenge when they attempt to apply good cybersecurity practices to their project management. Resource constraints prevent them from setting up security departments, and PMOs are metrics-driven rather than security-driven. Security is treated ad hoc and not integrated into projects to mitigate vulnerabilities; instead, it introduces new vulnerabilities. Enterprise security architectures are not suited for SMEs, nor are they aligned with project management approaches. What are the repercussions of not addressing this issue? This has been highlighted in reported incidents, including the HSE Ireland incident, which showed that known high-risk security problems had remained unresolved for more than 2 years due to governance issues and a lack of budget prioritization. In contrast, the MOVEit incident demonstrated a supply chain vulnerability spreading across the organization, with vendor security governance absent from its project process. There is an immediate need for an easy-to-use, lightweight tool that integrates security with project management for SME project managers and supports both Waterfall and Agile development cycles, with straightforward guidelines for project managers who do not specialize in security.

1.2. Research Questions

This research focus relates to the following three questions:

- What are the key challenges faced by SMEs in incorporating security within project management?
- How may effective integration of cybersecurity be achieved within Waterfall models and Agile development methodologies within SMEs?
- What are the mechanisms driving constant consideration of security within SME project portfolios?

Research Aim and Objectives: Based on the literature review and problem statements, a gap is evident, indicating a lack of a feasible, methodology-specific approach to integrating cybersecurity into the project management of small- to medium-sized enterprises. The research, as outlined in the following aim and objectives, addresses this gap.

Research Aim: The primary aim of this research is to develop a PMO-Led Cybersecurity Integration Framework that systematically embeds security governance into project management processes for small and medium enterprises. The framework addresses the documented need for security approaches appropriate for SMEs that respect resource constraints and provide meaningful protection [27]. Unlike existing enterprise frameworks that assume dedicated security teams and substantial budgets, this framework is designed for organisations with 10-250 employees, limited IT budgets, and no specialist security personnel. Following design science research principles, the framework creates a purposeful artefact to address the identified organisational problem, supporting both predictive (Waterfall) and adaptive (Agile) project methodologies through risk-proportionate controls [39].

1.3. Research Objectives

To achieve this aim, five specific objectives are established:

1. To identify cybersecurity challenges specific to SME project management contexts through a systematic literature review, examining security integration gaps in both predictive and adaptive methodologies. This objective addresses the research gap identified by Chidukwani et al. [4], who noted that SME-focused cybersecurity research remains limited, particularly in terms of practical implementation guidance.

2. To analyse real-world cybersecurity breaches and identify recurring project management failure patterns through case study analysis. This includes examining the HSE Ireland ransomware attack and the MOVEit supply chain breach, and extracting lessons applicable to SME governance contexts [5].
3. To develop a PMO-Led Cybersecurity Integration Framework comprising risk-proportionate security controls applicable to both Waterfall stage-gate and Agile sprint-based methodologies. This objective responds to Al-Janabi et al. [2] call for integrated cybersecurity and IT project management frameworks that address the persistent disconnect between security requirements and project delivery processes.
4. To validate the proposed framework through counterfactual analysis, examine whether its implementation would have prevented or mitigated the observed breach outcomes. This validation approach follows the FEDS framework for design science evaluation, providing a rigorous assessment where controlled experiments are impractical [20].
5. To provide actionable implementation templates enabling SME adoption without requiring specialist security expertise. This objective directly addresses the practical implementation gap identified by Valdés-Rodríguez et al. [36], who noted that existing frameworks lack actionable guidance for non-specialist project managers.

These five objectives collectively ensure that the research delivers both a theoretical contribution through framework development and a practical value through implementable templates for SME practitioners.

1.4. Scope and Limitations

Scope: The study focuses on SMEs, as defined by the European Commission, i.e., companies with 10-250 employees and budgets for IT projects of 100,000 to 2,000,000 pounds per year. The proposed framework considers projects totalling 5-30 in the active phase. The research paper will consider security in projects conducted under both Waterfall and Agile development processes, from initiation to decommissioning. The research paper views the PMO through the lens of security governance and as the central authority for security Integration.

Limitations: This study does not target large-scale companies that employ security professionals and operate sophisticated security operations centers, as their resource profiles differ fundamentally from those of the target SMEs. There will be no development of security tools. This study will continue to focus on processes. Industry-specific regulations are considered but not explored. This study will validate counterfactually through a case study rather than an empirical test in an SME environment. It should be performed in a future study. This study will use secondary sources rather than primary sources.

2. Literature Review

Most economies rely on SMEs as their backbone, yet, due to limited resources, expertise, and organizational maturity, they remain disproportionately vulnerable to cyber threats. With digital transformation gathering pace, SMEs are increasingly using technology to support operations, thereby exposing themselves to an expanding set of cyber risks. Cybersecurity is not generally visible in project management at an SME; in fact, security practices are either isolated to the IT function or not considered throughout the project life cycle [4]; [8]. This literature review covered three related topics: (1) the particular cybersecurity issues that SMEs face, (2) the use of project management techniques, especially predictive methods like Waterfall and adaptive methods like Agile/Scrum; and (3) integrating security procedures into project lifecycles. This assessment is motivated by the urgent need for SMEs to integrate cybersecurity into their project management processes. In light of the unique limitations and realities of SMEs, this review will examine how security can be successfully integrated across various project environments, including both Waterfall and Agile/Scrum approaches. With an emphasis on literature from 2019 to 2025, a thorough search was conducted across major academic databases. Peer-reviewed research, credible industry reports, and recorded case studies are given priority in this review, which focuses on workable solutions for SMEs. The objective is to identify research gaps that impede the creation of lightweight, SME-appropriate frameworks for security integration and to offer practical insights for SME project managers.

2.1. Cybersecurity Challenges in Small and Medium Enterprises

SME Characteristics and Constraints: The defining characteristics of SME, limited IT and security budgets, flat organizational structures, and multi-role employees determine the ability to implement measures of cybersecurity. Unlike large enterprises, most SMEs lack dedicated security personnel or a CISO. In fact, cybersecurity responsibilities in SMEs are often broadly distributed among non-specialist personnel who handle multiple tasks [8]. Resource constraints are persistent: SMEs cannot afford enterprise-grade security solutions or extensive staff security training, and the time required to implement and maintain complex security frameworks is often prohibitive given their limited resources. A lack of technical expertise further compounds the problem, as many SMEs have limited capacity to interpret and apply existing cybersecurity standards, which are written for organizations with greater resources and specialist personnel. Leadership in SMEs may also be unfamiliar with cybersecurity as a business enabler, viewing it instead as a cost centre or a purely technical issue rather than a strategic priority.

These constraints imply that SMEs seldom have the resources to engage a dedicated security project manager or a dedicated security project team. Security must therefore be integrated into existing project management roles and processes, using lightweight, low-cost approaches that fit the SME context. Security integration must be a part of how researchers do projects, not an additional or separate set of activities [4].

Threat Landscape and Impact: The threat landscape facing SMEs is equally wide and serious. The specific attack vectors include phishing and social engineering, ransomware, data breaches, supply chain attacks, malware, and DDoS attacks. SMEs are also connected to larger enterprises through the supply chain and therefore serve as an attractive entry point for attackers seeking to compromise a target of higher value [4]; [32]. The impact of cyber incidents on SMEs is disproportionate. Financial losses can be devastating, with some studies indicating that up to 60% of SMEs close within six months of a major breach. Beyond direct financial costs, SMEs suffer reputational damage, loss of customer trust, legal and regulatory penalties (such as those under GDPR), and significant business disruption. Many vulnerabilities are introduced during project implementation, especially when new systems or applications are deployed without adequate security measures. Thus, projects offer an important opportunity to integrate security from the start, as well as a source of new risks.

Current SME Security Practices and PMO Gap: Despite growing awareness of cyber risks, most SMEs adopt a reactive rather than proactive approach to cybersecurity. Security is often an afterthought, a reaction to incidents or external pressure. SMEs heavily rely on simple tools such as antivirus software and firewalls, while formal security policies or procedures are limited. This was pointed out by Emer et al. [8] and Chidukwani et al. [4]. There has been a sustained awareness-action gap, with several SMEs believing in cybersecurity but being either resource-starved or lacking the necessary skills and guidance to implement effective measures. In this respect, the chasm widens in the case of project governance. PMOs in SMEs are seldom in place and, when they exist, focus mainly on the so-called triple constraint of time, cost, and scope. Security is seldom explicitly addressed by any form of project governance. At the same time, risk management processes often confine security to an IT silo rather than integrating it into every project phase. Security requirements are seldom gathered during project initiation, and security testing is frequently deferred until after implementation—if it occurs at all. This results in minimal integration of security into project delivery processes, although projects are both a source of vulnerabilities and an opportunity to embed security. The literature reveals a significant gap: while there is extensive research on technical cybersecurity controls for SMEs and on project management methodologies, there is minimal research on their intersection—specifically, how to embed cybersecurity into project management processes for SMEs. Most secure SDLC research assumes enterprise resources and maturity, leaving SME project managers without practical, actionable guidance.

2.2. Security Challenges in Predictive Project Management (Waterfall)

The predictive or Waterfall project management methodology is a plan-driven, sequential approach wherein the project Phases-Requirements, Design, Implementation, Testing, Deployment, and Maintenance-are completed in order, with each phase building on the previous one. This model emphasizes comprehensive a priori planning, detailed documentation, and phase-gate reviews to support robust change control processes and make go/no-go decisions. In SMEs, the waterfall is often used for infrastructure projects, ERP/CRM implementations, compliance-driven projects, and hardware/physical system deployments. Its structured nature supports traceability and accountability, which are critical for many organizations to meet both external standards and internal governance needs.

Security in the Waterfall Lifecycle: Security integration at the Waterfall model should be ideally implemented at all stages, including requirements phase (identifying compliance mandates and conducting threat assessment), design stage (definition of a security architecture and control), implementation phase (securing coding practices), testing phase (vulnerability analysis and penetration testing), and deployment/maintenance phase (ensuring a secure configuration setup and patch management). In reality, security can be treated as an issue at the testing stage, leading to an expensive fix process, especially for fundamental design issues. SMEs face compounded challenges: double difficulties. For instance, without expert security professionals, security requirements cannot be comprehensively covered. In addition, a lack of capacity and skills limits the enforcement of best coding security practices. There are also difficulties in monitoring and intervening as security specialists due to a mismatch between capacity and requirements. The Waterfall model has implications for SMEs because, despite constantly changing threats, all stages must be revisited, which requires extensive documentation [14]; [15]; [23].

Integration Challenges and Gaps: There is a persistent gap between IT project management and cybersecurity requirements in traditional Waterfall approaches, especially in SMEs. The majority of the frameworks and standards either focus on risk management or secure coding but do not include a holistic, systematic integration of cybersecurity throughout the project lifecycle [2]. This can lead to the perception that security is an afterthought rather than an intrinsic part of project delivery. The lack of seamless integration is especially risky for SMEs, which typically operate on very limited security budgets and lack the expertise to proactively address identified vulnerabilities.

Emerging Frameworks: Recent frameworks indicate that cybersecurity risk management should be integrated into the IT project management lifecycle, with continuous, organized, and strategic security activities from the very beginning of a project through to decommissioning. In practice, such approaches have verified improved security postures in several real case studies, suggesting that even SMEs can benefit from adopting structured, lifecycle-based security integration [2]; [36].

2.3. Security Challenges in Adaptive Project Management (Agile/Scrum)

Agile project management has been characterized by iterative development, flexibility, and close collaboration among cross-functional teams. Compared to the sequential Waterfall model, Agile emphasizes short development cycles (sprints), continuous feedback, and adaptive planning. The generally accepted Agile frameworks are Scrum, Kanban, and Feature Driven Development (FDD); these are widely adopted, especially in dynamic environments where requirements evolve rapidly. For SMEs, Agile enables prompt response to market and customer needs, making it a very popular choice for software and IT projects alike [34]; [36].

Security Challenges in Agile Environments: Integrating cybersecurity into Agile presents its own set of challenges. Thus, in this quest for speed and adaptability, security gets left behind or considered at the end of development: Common issues include:

- Lack of dedicated security roles within Agile teams.
- Insufficient security requirements in user stories.
- Limited time for comprehensive security testing within short sprints.
- Cultural barriers between development and security teams.

They may especially lack the resources or skills to embed security practices, thereby making them more vulnerable to cyber threats.

Weaknesses and Challenges in Agile Project Management with Cybersecurity Integration: The rapid, iterative cycles typical of agile project management create tensions between speed and security; the need for speedy feature delivery may push security considerations to the side [24]. Because documentation in agile is limited, there is often a risk that security decisions are not properly documented. Hence, missed vulnerabilities could go unidentified, complicating tracking of security debt and of security tasks skipped or postponed [31]. Done is usually defined differently across teams and sprints; if no explicit security criteria are established, protection measures may be omitted. An Agile approach based on sprint-by-sprint focus fragments the view of the system-wide security architecture, complicating the coherence of security baselines and holistic threat management [1]. Continuous change and evolving requirements complicate maintaining a fully secure posture. Also, thorough threat modeling cannot be conducted iteratively, so proper risk assessment often remains incomplete. These challenges multiply for SMEs, as teams may lack security training, dedicated security roles, and/or access to automated security tools.

2.4. Security Integration Challenges in SME Project Management with Comparative Analysis on Predictive vs Adaptive Security

A comparative analysis of predictive and adaptive approaches to cybersecurity integration is presented, highlighting their distinct strengths and trade-offs across key project management dimensions. Table 1 below summarizes these differences based on Al-Janabi et al. [2] and PMBOK 7th Edition:

Table 1: Side-by-Side comparison of security Integration in Predictive vs Adaptive Project Management

Dimension	Predictive (Waterfall)	Adaptive (Agile/Scrum)
Security Timing	Upfront planning (requirements, design)	Continuous, every sprint
Security Discovery	Testing phase (late)	Throughout development (early)
Threat Modeling	Comprehensive, upfront (design stage)	Iterative, sprint-level
Requirements	Documented in the requirements phase	Security user stories in backlog
Testing	Dedicated testing phase	Continuous, automated in CI/CD
Reviews	Phase-gate reviews, formal sign-offs	Sprint reviews, demos, retrospectives
Documentation	Comprehensive (specs, plans)	Lightweight (stories, criteria)
Change Management	Formal control (changes are costly)	Flexible (adapt in next sprint)
Accountability	Phase owners responsible	Whole team (collective ownership)
Cost of Late Fixes	Very high (10–100x)	Lower (fix in next sprint)
Security Debt	Front-loaded (in planning)	Can accumulate if unmanaged
Best for SMEs	Regulatory/compliance, fixed scope	Software development, evolving needs

Predictive or Waterfall approaches structure security into distinct phases that require significant up-front expertise, planning, and documentation. Security requirements, threat modeling, and testing are handled early and in a highly formal manner, which is beneficial for projects with stable requirements and strict regulatory or compliance requirements. This model typically uncovers security issues very late in the process, which can be costly to fix and may create vulnerabilities when requirements change mid-project. On the other hand, adaptive approaches (such as Agile/Scrum) incorporate security activities throughout the development life cycle. Security is addressed iteratively through user stories, continuous testing, and periodic reviews, enabling early detection and rapid remediation of vulnerabilities. Agility allows teams, on the one hand, to adapt to evolving requirements and new threats but, on the other hand, brings in many risks: fragmented security architecture, inconsistent documentation, accumulation of security debt if the prioritization of security is not explicitly set up each sprint Agile is best applied in SMEs involved in software development or innovation projects where the requirements are fast-evolving and speed is of essence. Neither approach is inherently more secure; both approaches can provide robust security if security integration is intentional and explicit. The best choice will depend on the project context: Waterfall is a better fit for compliance-driven, fixed-scope projects, while Agile is better for projects that require quick delivery and adaptability.

2.5. Existing Frameworks and Limitations for SMEs

SDLC Frameworks: Secure SDLC frameworks are critical in embedding cybersecurity into project management, but most are designed for large organizations and pose several challenges for SMEs. This includes complete security integration, though it assumes dedicated security teams and thus requires considerable resources. Microsoft SDL is an enterprise-grade framework that provides comprehensive guidance on security activities, ranging from training to response. However, it assumes significant resources and dedicated security teams and tends to be resource- and process-intensive for small teams. Most SMEs lack the capacity for such elaborate processes, which explains the difficulties in adopting security practices [17]. NIST SP 800-218, the Secure Software Development Framework (SSDF), provides 42 guidelines across four stages: Prepare the Organisation, Protect the Software, Produce Well-Secured Software, and Respond to Vulnerabilities [22]. While very detailed and gaining acceptance in the public sector and in controlled industries, the documentation requirements and maturity levels appear to exceed the capabilities of many SMEs. OWASP SAMM is an open-source and Agile-compatible Software Assurance Maturity Model structured by themes of governance, design, implementation, verification, and operations. However, while flexible, SAMM might still be too intricate for SMEs because it requires some security expertise to interpret and apply maturity assessments, which can overwhelm small teams. Most secure SDLC frameworks are designed to assume dedicated security resources, enterprise-scale complexity, and significant investment. They do not consider specialized project management methodologies or the peculiarities of SMEs, and they often lack actionable items for a project manager who is not a security expert [36]. This results in limited use and effectiveness in smaller organizations.

General Cybersecurity Frameworks: While general cybersecurity frameworks such as the NIST Cybersecurity Framework, ISO 27001/27002, and CIS Controls are widely recognised and can strengthen SME security posture, each has notable limitations for integration into project management. The NIST CSF organizes security into five functions: Identify, Protect, Detect, Respond, and Recover. Although flexible and efficient for risk management, it is not designed to integrate directly into the project lifecycle; hence, it is difficult to apply in practical SME projects [12]. ISO 27001/27002 offers a comprehensive ISMS and a catalogue of controls, yet the standard's organisational focus and the high costs of certification limit its applicability to SMEs, particularly for project-specific requirements. CIS Controls provide 18 prioritized technical controls, among which IG1 applies to SMEs. However, these controls focus on technical measures rather than on integrating a project management process. Overall, these frameworks can inform SME security objectives but require adaptation for effective project-level integration.

Project Management Security Guidance: Project management standards, such as PMI's PMBOK, provide only slight explicit security guidance; if anything, security is addressed under the umbrella of risk management rather than as a focus across project phases [2]. The Scrum Guide, one of the most widely used guides in Agile environments, does not make any explicit security provisions. Therefore, teams lack structured security practices [3]. This leads to the identification of a key gap: limited specific guidance by major project management bodies on embedding security at all stages of the project life cycle, particularly for SMEs. Recent research has identified a need for an integration layer that links cybersecurity frameworks to project management methodologies within SMEs, ensuring that security considerations are systematically addressed from project initiation to closure.

3. Methodology

3.1. Research Philosophy: Pragmatism

The approach in this research is Pragmatism, which is the established paradigm for Design Science Research (DSR) in general. In Pragmatism, knowledge is validated by its utility in solving real-life problems rather than by aiming for truth or subjective

meaning [11]. In this case, this perspective is relevant, as the first criterion for success is whether this framework can address SME cybersecurity governance failures. In contrast to positivism, which pursues universal laws, and interpretivism, which focuses on the meaning of things, pragmatism emphasizes what works in particular circumstances [39]. Such an approach tends to align well with the idea of building a framework that can be easily implemented while also respecting the context-dependent nature of SME cybersecurity practices across different-sized enterprises and sectors.

3.2. Research Approach

Design Science Research: This study follows the DSR approach, focusing on the development and testing of artefacts to address identified organizational issues. In this case, it is appropriate because DSR aligns well with the artefact-driven objective of this research: the development of a PMO-Led Cybersecurity Integration Framework that addresses the documented gap in cybersecurity governance for SMEs. In this respect, the DSR method follows a process of pinpointing the problem through a systematic review of the literature and an analysis of the case study, designing the artefact by combining frameworks into a new architecture, and evaluating it. Specifically, the approach mixes deductive elements, in the sense of bringing established theories and standards into the setting of the SMEs, with a design-focused logic rather than purely theory testing.

3.3. Research Strategy

The nature of this study aligns with the qualitative, descriptive, and analytical research strategy in accordance with Design Science Research. This study adopts a qualitative, descriptive, and analytical research strategy. Qualitative research focuses on non-numerical data to understand meanings, patterns, and the ‘how’ and ‘why’ behind phenomena, making it well-suited to exploring complex organisational contexts. The descriptive element documents the current state of cybersecurity practices in SMEs, identifying what is in place and what is missing. Analytical methods involve critical evaluation, comparative analysis, and synthesis to identify gaps and generate actionable insights.

3.4. Research Methods

This research employs two complementary methods: a Systematic Literature Review (SLR) and Case Study Analysis. The SLR establishes theoretical foundations and identifies knowledge gaps, while case studies provide real-world evidence to validate and contextualise them. Together, these methods ensure both rigour and practical relevance in addressing SME cybersecurity integration within project management. Cases sourced from government investigation (NCSC, CISA), industry reports (Verizon DBIR), and academic journals.

Method 1: Systematic Literature Review: The first method employed in this research is a systematic literature review (SLR), which aims to provide a comprehensive understanding of cybersecurity challenges faced by small and medium-sized enterprises (SMEs), analyze the integration of security practices within Waterfall and Agile project management methodologies, evaluate existing frameworks, and identify critical gaps in current knowledge. The SLR follows established protocols, such as PRISMA, to ensure rigour and transparency in the identification, screening, and selection of relevant studies. The search strategy encompasses major academic databases, including IEEE Xplore, ScienceDirect, Wiley, Springer, the PMI Digital Library, and industrial standards from NI ST, ISO, and OWASP. The review uses a combination of primary keywords—such as SME cybersecurity, project management security, and secure SDLC—and secondary terms, including Agile security, Scrum security, Waterfall security, and DevSecOps. Boolean operators are applied to refine the search, focusing on literature published between 2019 and 2025, with a particular emphasis on the most recent studies. Inclusion criteria are strictly defined to ensure the quality and relevance of the selected literature. The selection process begins with an initial pool of over 100 papers, which is narrowed through title and abstract screening to approximately 60 studies. A full-text review further refines the selection, yielding a final set of over 30 papers prioritised by recency, relevance, methodological rigour, and credibility.

Method 2: Case Study Analysis: To complement the theoretical insight from the literature review, this research uses case study analysis. Although the research targets SMEs, in selecting case studies, the research prioritizes governance failure transferability over adherence to a strict employee count threshold:

- **HSE Ireland:** Despite its size, HSE Ireland reflects the governance problems found in smaller firms: decentralised project teams with 10 to 50 participants, without security oversight by a centralised PMO, a security budget subordinate to operational needs, and a High Risk rating that has remained unaddressed for 2 years. The level of information provided by Sulaiman et al. [26] on project governance failures is highly informative compared to what might be expected from other smaller-entity breach notifications.
- **MOVEit Supply Chain Breach:** This scenario is relevant to SMEs that have implemented MOVEit for affordability and compliance reasons, as illustrated by their failure in vendor risk assessment, ad hoc patch management, and a lack of monitoring by a third-party entity.

SME breaches tend to resist detailed incident reporting because they cannot afford to conduct post-event analyses. The patterns of failure that have been observed: invisible risk, unfunded security, and unclear ownership, have been noticed to occur, independently of organisational size, where similar gaps exist within their governance structures. Every case is evaluated through a systematic seven-step process: context establishment, impact description, timeline mapping, root cause analysis, mapping to PM standards, pattern recognition, and framework applicability evaluation.

3.5. Data Collection

Only peer-reviewed journal articles, conference proceedings, and reputable industry or government reports (such as those from NIST, PMI, OWASP, and Verizon) published in English within the specified timeframe are considered. Studies that focus exclusively on large enterprises, describe purely technical tools without a broader context, present opinion pieces, or are not available in English are excluded. Reference management is handled with Zotero, featuring browser integration, cloud synchronisation, and thematic tagging for efficient retrieval. The extracted literature is organized in Excel matrices that capture author, year, title, findings, research gaps, and PEER notes, with colour-coded themes for clarity. Case documentation employs structured templates, timeline diagrams, and root cause analysis notes, ensuring consistency and depth. All data is securely stored on OneDrive with password protection and two-factor authentication, backed up on an encrypted external drive, and version-controlled through dated files.

3.6. Data Analysis

Literature Analysis Techniques: Thematic analysis is applied to the literature, coding and grouping findings into six core themes: SME challenges, Waterfall security, Agile security, comparative analysis, frameworks, and research gaps. Sub-themes are developed iteratively, with the PEER method and PMP knowledge informing the identification of patterns and relationships. A comparative analysis is conducted between the Waterfall and Agile methodologies across more than 20 dimensions, using a matrix to systematically assess their strengths and weaknesses. Gap analysis identifies explicit, implicit, practical, and methodological gaps, which are then categorized and prioritized to inform future research directions.

Case Study Analysis Techniques: Within-case analysis involves a detailed examination of each case, including timeline mapping, applying the 5 Whys root cause technique, mapping project management failures to PMBOK or Scrum standards, and extracting key lessons. Cross-case analysis identifies patterns across all cases, quantifies the frequency of common failure points and root causes, and examines recurring methodology patterns. This approach validates the proposed framework design and ensures that findings are robust and generalizable to SME project management contexts.

3.7. Ethical Considerations

Ethics approval is not required for this study, as it involves only secondary data and no human participants. Ethical practices include proper citation (Harvard style), avoidance of plagiarism, compliance with copyright laws, respect for anonymity, secure data storage, and a data destruction plan. The research fully complies with university policy, GDPR, and the Data Protection Act, ensuring responsible and ethical handling of all data sources.

3.8. Reliability and Validity

Reliability is ensured through a systematic, transparent process that includes documented search strategies, clear selection criteria, and detailed case selection. An audit trail is maintained using matrices, structured templates, version control, and supervisor reviews. Triangulation—drawing on over 30 papers, multiple cases, and diverse sources—minimises bias and enhances consistency. Validity is strengthened by prioritizing high-quality, peer-reviewed, and reputable sources, with credibility assessments for each. Triangulation across multiple papers, integration of literature and case studies, and the combination of theory with practice further enhance validity. Critical analysis is conducted using the PEER method, with explicit acknowledgement of limitations and discussion of conflicting findings. Regular supervisor feedback provides additional validation and helps ensure the integrity of the research process.

3.9. Limitations of the Methodology

This study's exclusive reliance on secondary data means its findings cannot be directly validated with real SME project managers; however, using diverse, reputable sources and recommending future primary validation helps mitigate this limitation. Case selection is constrained, often biased toward failures, and limited in sample size, but focusing on patterns rather than statistics and using credible documentation addresses this. The conceptual framework has not been empirically pilot-tested; future research should conduct pilot studies to assess its practical validity. Finally, the limited project duration restricts the scope, but clear boundaries and recommendations for future research help manage this.

3.10. Researcher Positionality

The researcher's background includes PMP certification and over nine years of experience (split between telecom and project management), providing strong PM knowledge and familiarity with PMBOK and SME contexts. This expertise offers insider strengths for developing practitioner frameworks but may introduce PM-centric or telecom-related biases and a preference for structured approaches. Systematic protocols and regular supervisor review are used to mitigate these biases, ensuring transparency and rigour.

4. Finding and Analysis

- **SME Resource Constraints:** Small and medium enterprises face persistent resource constraints that limit their cybersecurity capabilities. Surveys and reviews consistently report limited financial resources, lack of skilled security staff, and low cyber-risk awareness, leaving SMEs reliant on non-specialist personnel and outdated technologies. Empirical studies show that many SMEs cannot afford enterprise-grade tools, struggle to maintain formal policies, and underinvest in IT infrastructure, despite clear links between IT investment and cybersecurity readiness [19]. These constraints reinforce the need for lightweight, prioritised security controls tailored to SME capacity rather than enterprise-style security functions.
- **PMO–Security Gap:** A structural disconnect exists between project governance and cybersecurity. Research on cybersecurity governance and enterprise risk management emphasises that treating security as an isolated IT function weakens risk visibility and limits its integration into strategic decision-making. Project management–oriented work highlights that mainstream PM standards (e.g., PMBOK) mention security but lack concrete mechanisms for embedding it into project lifecycles, leaving project success vulnerable to cyber incidents. Conceptual models argue that project managers and project governance structures should explicitly own cybersecurity capabilities. Yet, current maturity models and ERM practices rarely operationalise this at the project or PMO level.
- **Waterfall Security Challenges:** Security integration in predictive lifecycles is frequently deferred to late phases. Studies on secure software development in traditional or policy-driven Waterfall models note that security is often considered only at testing or post-deployment, leading to late vulnerability discovery and costly rework when design decisions must be revisited. While phase-gate models can support traceability and structured control, they presuppose substantial upfront security expertise and systematic policy definition, which many SMEs lack.
- **Agile Security Challenges:** In Agile and DevOps/DevSecOps contexts, the main tension lies between delivery speed and security rigour. Systematic reviews of DevSecOps adoption and secure Agile development report that rapid iteration, feature-focused backlogs, and continuous deployment practices tend to sideline structured security work, fragment architectural oversight, and generate security debt. Limited documentation and emphasis on minimal artefacts further complicate traceability of security decisions, particularly in SMEs that already operate with constrained expertise and capacity.
- **Existing Framework Limitations:** Enterprise security frameworks such as NIST CSF and ISO/IEC 27001 are widely recognised and effective in larger organisations. Still, their adoption in SMEs is uneven due to complexity, resource demands, and the generic nature of their guidance. Reviews of NIST CSF implementation show that SMEs struggle, especially with the Detect, Respond, and Recover functions, reflecting a lack of capacity to operationalise the full lifecycle of controls. Case studies and SME-focused frameworks argue that existing standards are not sufficiently tailored to SME contexts, often require external consultancy, and are not aligned with project management practices, leaving project managers without actionable, methodology-specific guidance.

Collectively, these findings reveal a critical gap in current knowledge and practice: no practical, methodology-specific security integration framework exists for SME PMOs that addresses both Waterfall and Agile contexts while respecting resource constraints and governance realities. This gap, combined with the empirical case study analysis presented in Sections 4.2 and 4.3, directly informed the design principles and components of the PMO-Led Cybersecurity Integration Framework.

4.1. Case Study Analysis

4.1.1. HSE Ireland Ransomware Attack: Case Study Analysis

Organization Setting: Health Service Executive (HSE) Ireland, the national public health service with approximately 130,000 employees, operated IT through a decentralized structure with SME-sized project teams. From 2019 to 2021, HSE undertook several IT modernization projects, including infrastructure upgrades, electronic health record (EHR) implementations, and cloud migrations. Despite cybersecurity being rated High Risk since Q1 2019, the National Healthcare Network remained entirely unsegmented—a flat network design—representing a fundamental security infrastructure gap [28].

Incident and Impact: On May 14, 2021, the Conti ransomware attack encrypted 80% of HSE's IT environment (over 2,800 servers and 3,500 workstations) following eight weeks of the attacker's presence, initiated by a phishing email on March 18, 2021. The unsegmented network enabled lateral movement, compromising seven hospitals. The impact included a nationwide health system shutdown, delayed cancer treatments, and significant patient safety risks. HSE refused a $20 million ransom; recovery took over 4 months, aided by a decryption key from the attackers.

PM Failure Analysis: PMO governance failures were identified, including the absence of centralized cybersecurity oversight, the lack of a network segmentation project despite a High Risk status, and the consistent deprioritization of security infrastructure in favour of business features [29]. The root cause was a lack of mechanisms to ensure that high-priority risks translated into funded projects, leaving critical vulnerabilities unaddressed.

Key Lesson and Framework: High-risk items in the risk register must automatically trigger the initiation of security projects, ensuring that critical vulnerabilities are addressed rather than remaining as passive documentation. Foundational security infrastructure—such as network segmentation, patch management, and monitoring—must be protected in the budgeting process and not forced to compete with business features for funding. A PMO-driven framework with a portfolio security dashboard, risk-to-project processes, mandatory security budget allocation, and annual portfolio security reviews would have forced timely action.

4.1.2. MOVEit Supply Chain Attack: Case Study Analysis

Organisation Setting: MOVEit Transfer, developed by Progress Software/Ipswitch, is a managed file transfer (MFT) solution used by over 3,000 organisations worldwide. SMEs were drawn to MOVEit for compliance (HIPAA, GDPR, PCI-DSS) and affordability compared to custom solutions. Between 2020 and 2023, MOVEit was integrated into digital transformation projects, including cloud migrations and ERP deployments. The critical CVE-2023-34362 zero-day SQL injection vulnerability was exploited before the patch release. SMEs typically deploy MOVEit as a turnkey infrastructure, focusing on functionality rather than security validation. Key gaps included a lack of SOCs, vendor risk management, and post-deployment monitoring.

Incident and Impact: On May 27, 2023, the Cl0p group began exploiting the MOVEit zero-day, four days before a patch was available. Progress Software released emergency patches on May 31, but mass exploitation continued until June 15. Over 2,700 organizations across 60 countries and 93 million individuals were affected, including high-profile victims such as the U.S. Dept of Energy, British Airways, and Zellis. SMEs faced GDPR fines (£50k–£500k), incident response costs (£75k–£250k), weeks of disruption, insurance premium hikes, and customer churn. CISA's Emergency Directive ED 23-02 revealed widespread asset management failures, with many SMEs discovering untracked MOVEit instances.

PM Failure Analysis: The attack unfolded in three phases: exploitation (LemurLoot web shell, SQL injection, Azure Blob credential theft), exfiltration (PII and financial data via encrypted channels), and extortion (data ransom targeting compliance fears). Four PMO governance failures emerged which align with the three meta-patterns identified across cases: (1) No vendor security in project lifecycles (invisible risk); (2) Patch management was ad hoc, with no formalized, resourced process (unfunded security); (3) No third-party risk monitoring (invisible risk); (4) Supply chain security was absent from project gates (unclear ownership/governance). The root cause: PMO frameworks assumed full internal control, ignoring the reality that 60–80% of SME infrastructure depends on third-party solutions.

Key Lessons and Framework Implications: SME PMOs must embed vendor security as a mandatory project gate, formalize patch management as a standing project, implement continuous third-party risk monitoring, and integrate supply chain security into stage-gate methodologies. This framework addresses the SME governance gap, ensuring third-party dependencies receive robust security oversight—critical for organizations with limited internal resources.

5. Framework Development

A PMO-led Cybersecurity Integration Framework was developed by synthesizing two complementary approaches. Firstly, a systematic literature review showed that existing cybersecurity frameworks for SMEs are fundamentally flawed, as enterprise-standard frameworks such as NIST CSF and ISO 27001 presuppose budgets that SMEs do not have. There is a need for effective implementation practices for cybersecurity integration in PM that can be adapted for SMEs with limited budgets, something that frameworks such as those suggested by Al-Janabi et al. [2] or Harake [13] do not achieve. Second, the analysis of empirical cases through study research examined large-scale cybersecurity breaches: HSE Ireland (loss of €100M+, recovery time: 4 months) and the MOVEit attack on the supply chain (2,700+ organizations, 93 million individuals). These were classified into three meta-weaknesses: failure in initiation and planning, failure in execution and monitoring, and failure in resource allocation and prioritisation. This development of a framework adopts a design science research (DSR) paradigm, which focuses on developing a meaningful artefact to resolve recognized issues within an organization [7]; [39].

DSR provides a robust means of developing prescriptive solutions with practical relevance, while maintaining academic rigour. Upon development, validity is established using the FEDS framework through counterfactual analysis with documented instances, effectively investigating the potential of the framework's deployment to prevent or reduce observed violations [38]. Instead of supplanting existing standards, the framework takes best practices from NIST SP 800-30 (Risk Assessment), ISO 27001 Annex A.15 (Supplier Relationships), NIST SP 800-40 (Patch Management), and COBIT 2019 (Governance) and distils them into actionable, small-enterprise-ready processes. This framework is aimed at SMEs employing between 10 and 250 staff, with limited budgets, supporting between 5 and 30 live projects. It applies to both Waterfall and Agile development methodologies, from inception through to product decommissioning, with projected overheads of 12-34 hours, depending on risk category.

5.1. Design Principle

Five evidence-based principles anchor this framework. Each responds directly to documented breach failures and addresses known gaps in the literature:

- **Embedded, Not Additional:** This tenet extends the PCI Security Standards Council [25] guidance on integrating with SDLC to a broad application encompassing any type of project, including infrastructure projects and vendor development. The HSE example showed that a separate security governance framework creates accountability issues, with security concerns documented but not necessarily addressed. It has been verified that bolt-on security measures are ineffective in resource-limited settings [27].
- **Risk-Proportionate Governance:** A risk classification scheme with a three-tier structure (HIGH/MEDIUM/LOW) is based on the NIST SP 800-30 approach to conducting a risk assessment using a two-dimensional Likelihood × Impact matrix, tailored for SMEs [16]; [21]. This is a response to the literature insight that SMEs would be hampered if enterprise security standards were applied to all projects. Therefore, it advocates a risk-proportionate approach, in which security measures are scaled to each project's specific risk level.
- **Forcing Functions Over Optional Checkpoints:** Mandatory gates with blocking mechanisms replace optional security checkpoints. The war of attrition documented in the HSE case, in which security always lost to other demands, shows that an advisory approach does not work. This principle concerns the same issue that Harake [13] identified in security integration: that it is only possible with a governance framework that has enforcement power.
- **Continuous Over Point-in-Time:** Standing security projects maintain ongoing protection rather than relying solely on project-phase assessments (point-in-time), thereby supporting organisational cyber resilience. The MOVEit attack occurred through a software production vulnerability that could not be established within a point-in-time framework.
- **Methodology-Agnostic Design:** This framework supports either the Waterfall stage-gate development methodology or Agile development methodologies, as hybrid methodologies are often used by SMEs. DevSecOps tenets guide the design of the Agile elements by integrating security into their ceremonies and pipelines [10]; [6].

5.2. Framework Architecture

It comprises twelve elements that are grouped into four functional families:

- **Group 1:** Waterfall Security Integration (FR-01 to FR-05). Stage-gate security controls are aligned with the classic project phases.
- **Group 2:** Agile Security Integration (FR-06) Sprint-based security tasks for iterative development approaches.
- **Group 3:** Standing Security Projects (FR-07 to FR-08) Activities related to monitoring and maintenance that do not depend on projects.
- **Group 4:** PMO Governance (FR-09 to FR-12).

Portfolio-level governance, reporting, and budgeting safeguards. This framework is unique among other models in identifying the PMO as the governing body, rather than sharing security responsibility among various project teams, reflecting the shared accountability observed in both the HSE and MOVEit scenarios (Figure 1).

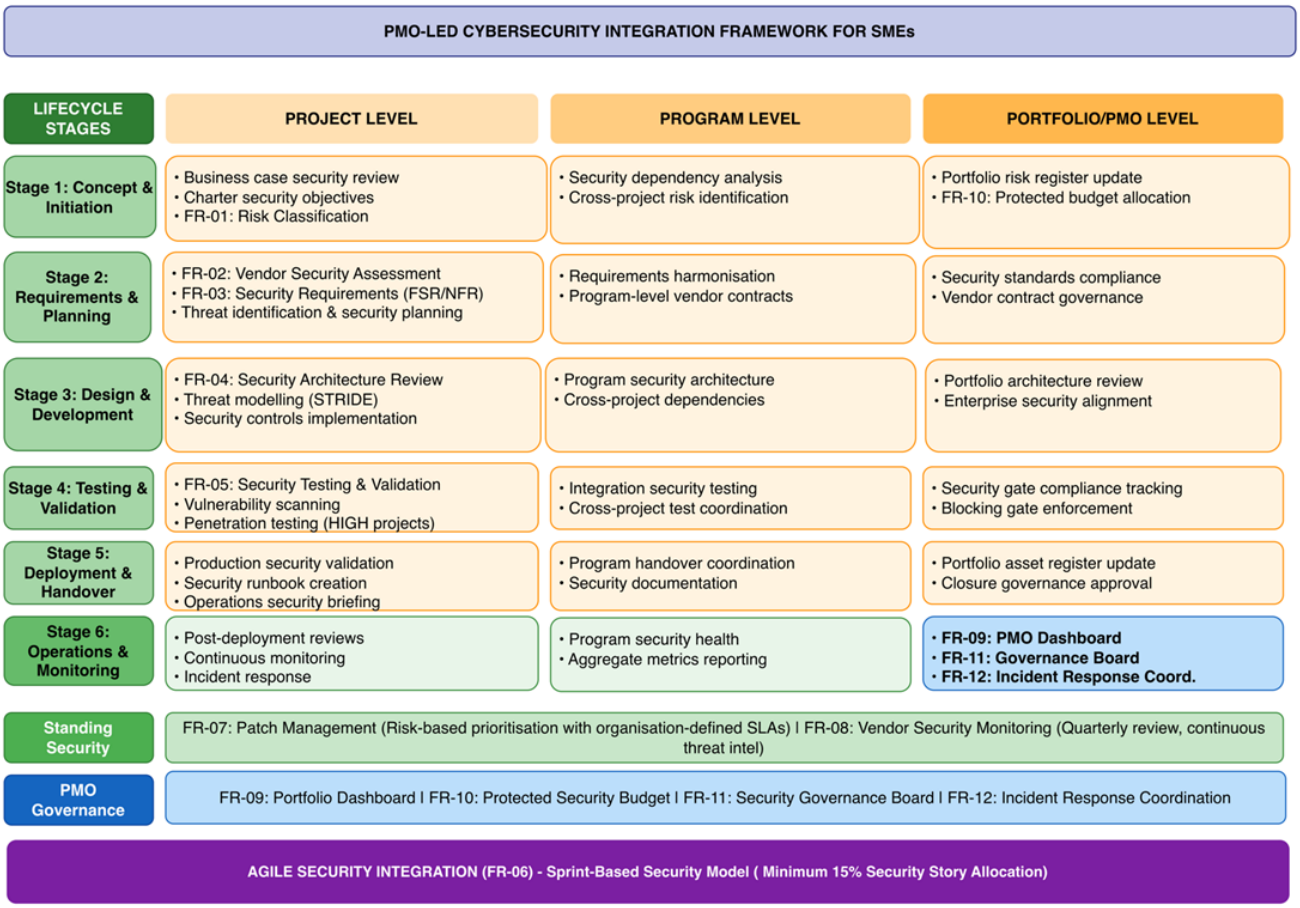

Figure 1: Framework architecture matrix

5.3. Framework Components

5.3.1. Group 1: Waterfall Methodologies Security Integration

Components of security gates align with the Waterfall project stages, ensuring security considerations are addressed before progressing to the next stage (Figure 2).

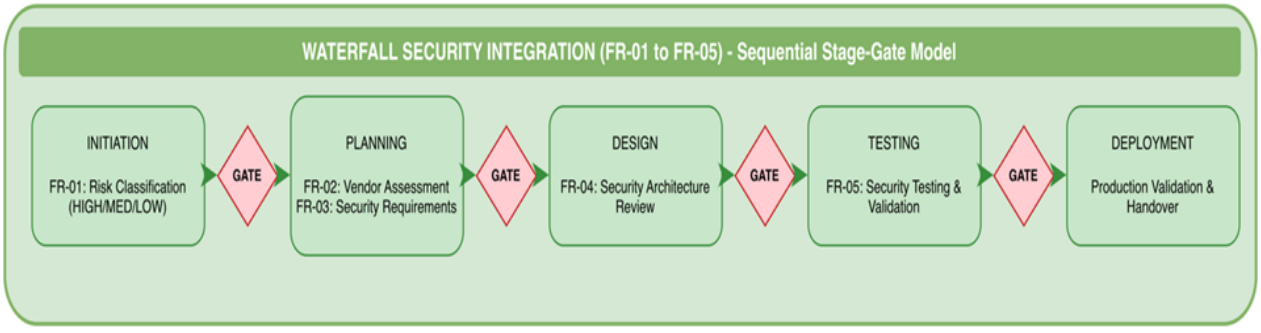

Figure 2: Waterfall project management security integration

FR-01: Security Risk Classification (Initiation Gate): FR-01 implements the risk assessment procedure per NIST SP 800-30 guidelines, with an approach scaled for SMEs. Using a two-dimensional risk analysis (Likelihood × Impact), security requirements for gates are established through a three-level categorization system (HIGH/MEDIUM/LOW).

Assessment Methodology: Part A: Threat Likelihood – identifies Exposure Factors (Data sensitivity, internet exposure, third-party dependencies, regulatory scope). **Part B:** Business Impact - Examines possible outcomes (financial, business, reputation, regulatory):

Risk Likelihood Level × Impact Level -> Classification Score =

Implementation: Security Risk Classification Form to be done by the Project Manager during the development of the project charter. The PMO will then verify this within 48 hours.

Time Requirement: 2-4 hours (HIGH), 1-2 hours (MEDIUM), 30 minutes (LOW).

FR-02: Vendor Security Assessment (Planning Gate): The mandatory vendor security assessment for projects that include third-party vendors or other external integrations is intended to address vulnerabilities in the software supply chain exploited in the MOVEit attack. Supply chain compromise is one of the key threat vectors affecting organisations of any size, according to the ENISA Threat Landscape 2025 [9]. This solution leverages ENISA's threat intelligence to inform executable assessment criteria assessment components:

- Review of Security certification (ISO 27001, SOC 2)
- Data processing and breach notification practices
- Security requirements in contracts and SLA commitments
- Critical services dependency map creation

Implementation: Vendor Assessment Checklist accomplishments before vendor contract execution. Vendors with a HIGH risk need PMO Approval.

Time Requirement: 4-8 hours per vendor (initial), 2 hours per vendor (annual renewal).

FR-03: Security Requirement Specification (Planning Gate): Integrating security requirements with project requirements is important to ensure security is considered alongside other functional requirements rather than addressed at the end. This is one of the areas that contribute to the planning failure mentioned in the HSE case analysis requirement categories:

- Authentication and authorization needs
- Data encryption and processing needs
- Logging and Audit Trail Requirements
- Compliance regulations (GDPR, industry-specific)

Implementation: The Security Requirements Template is incorporated into project requirements documentation. Traceability of security requirements to security controls is achieved during the design phase.

Time Requirement: 4-8 hours (HIGH), 2-4 hours(MEDIUM).

FR-04: Security Architecture Review (Design Gate): A technical security review of the proposed architecture is used to ensure that security measures are built into solutions rather than added after the fact. This reflects the current state of technical debt accumulation in HSE infrastructure review components:

- Network segmentation and access controls
- Data flow analysis, encryption needs
- Integration security (APIs, data exchanges)
- Compliance verification
- Defense in depth that avoids a single point of failure

Implementation: The Architecture Security Checklist is used during the design review. For projects with HIGH risk, an independent security review is necessary.

Time Requirement: 4-6 hours (HIGH), 2-4 hours (MEDIUM).

FR-05: Security Testing and Validation (Deployment Gate): Security validation before deployment ensures that vulnerabilities are identified and addressed before deployment to production. This is an area that addresses execution failures related to vulnerabilities that were recognized but left unchecked, testing activities:

- Vulnerability scanning (automated)
- Penetration testing (HIGH risk projects)
- Configuration compliance verification
- Security run-book validation

Implementation: Testing results recorded in the Security Validation Report. Blocking vulnerabilities (Critical/High severity) need to be fixed before deployment approvals.

Time Requirement: 6-10 hours (HIGH), 3-5 hours (MEDIUM), 1-2 hours (LOW).

5.3.2. Group 2: Agile Project Management Security Integration

While FR-01 through FR-05 map Waterfall governance principles into security, FR-06 does the same for Agile methodologies. This is a testimony to the security governance framework's methodology-agnostic approach [10].

FR-06: Sprint Security Integration: FR-06 translates the principles of DevSecOps in the enterprise into small-business applications, incorporating the work of Sharma and Bawa [30] on identifying security activities.

Integrating security into Agile development requires embedding structured security activities across all sprint phases. During sprint planning, teams should allocate at least 15% of sprint capacity to security-related user stories in the product backlog, treating security as a core development priority rather than an afterthought. This phase should also include lightweight threat modelling of new features, such as STRIDE analysis, to proactively identify potential risks, as well as clearly defined security acceptance criteria for each user story. During sprint execution, security practices must be continuously enforced through automated security scanning integrated into the CI/CD pipeline, including static application security testing (SAST). High-risk changes should undergo dedicated security code reviews to identify vulnerabilities early, while an ongoing vulnerability monitoring process ensures timely detection and mitigation of emerging threats. Finally, during the sprint review and retrospective, teams should evaluate security performance by reviewing key metrics, such as the vulnerabilities introduced and resolved during the sprint. Security debt should be analysed and prioritised in the backlog to maintain long-term system resilience. Additionally, capturing lessons learned from any security incidents helps improve future practices and strengthens the overall security posture of the development lifecycle.

Quarterly Security Sprint: In every fourth sprint, security work such as penetration testing, security debt fixes, or updates to security tools is prioritised, with 80 per cent capacity utilisation. Hence, the idea of a security sprint prevents the buildup of security debt to levels that could be difficult to tackle.

Implementation: Additionally, the Agile Security Integration Guide in this work includes detailed integration ceremonies. The PMO security training is given to the Scrum masters.

Time Requirement: Continuous, about 15-20% of the total team capacity devoted to the sprint.

Sprint Security Allocation Flexibility: The 15% minimum allocation accounts for the fact that inflexible allocations may not always be applicable in some sprint situations. The following flexibility situations allow for adaptation based on context concerning security responsibility (Table 2):

Table 2: Sprint security allocation flexibility scenario table

Scenario	Minimum Allocation	Condition	Approval Required
Standard	15–20%	Default for all regular sprints	None
Carryover Credit	10%	Previous sprint achieved ≥25% security allocation, and the current security debt is zero.	Not required
Security Complete	5%	All functional and non-functional security requirements implemented, security testing passed, and no outstanding HIGH/CRITICAL findings.	PMO approval required

Emergency Outage	0%	P0/P1 production incident requiring full team capacity; compensatory sprint must allocate minimum 30%	Executive approval required
Maintenance Only	10%	Sprint contains no new features, no attack surface changes, bug fixes only	Not required
Quarterly Security	80%	Every fourth sprint is mandatory: penetration testing, security debt elimination, and training.	Mandatory (no exemption)

No sprint planning can begin without either (a) satisfying minimum security allocation for a given scenario, or (b) an approved exception with a compensatory plan in place. The PMO Dashboard (FR-09) highlights trends in sprint security allocation, and projects with chronic under-allocation (three or more sprints below the minimum without an approved exception) will be escalated for attention.

CI/CD (Continuous Integration/Continuous Deployment) Pipeline Security Integration: For teams with continuous integration infrastructure in place, security controls are integrated into their deployment pipelines, as shown in Figure 3. Pipeline security gates will prevent deployment if Critical or High-severity vulnerabilities are discovered. A team without a CI/CD implementation can establish a security gate in its SDLC process.

Tool Recommendations (SME-Appropriate): Free/Open Source solutions suitable for resource-constrained settings:

- OWASP Dependency-Check (Software Composition Analysis)
- SonarQube Community Edition for Static Application Security Testing
- Trivy (Scans Containers and Infrastructure)
- Git-secrets (Credential Detection)

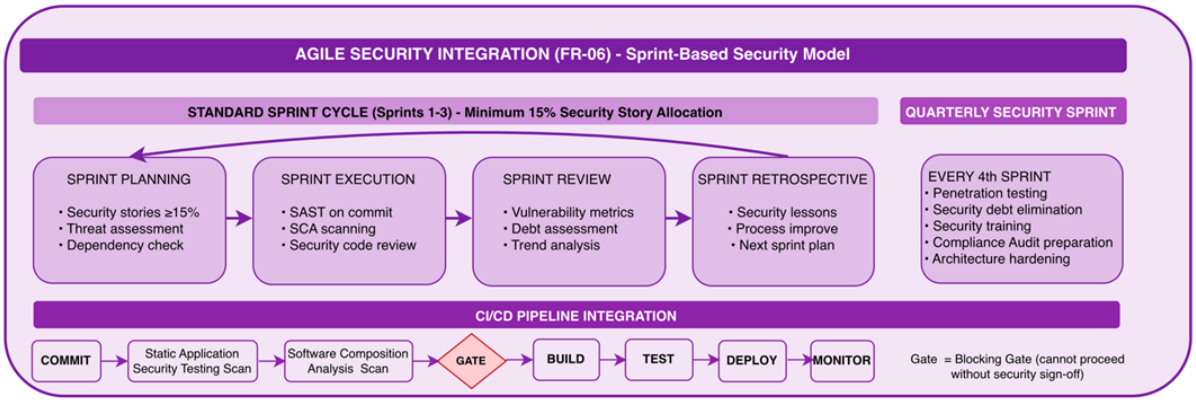

Figure 3: AGILE and CI/CD pipeline integration

5.3.3. Group 3: Standing Security Projects

The standing security elements run continuously and independently of project cycles, filling a gap when security threats arise interstitially, between project phases. What is "Standing"? In here, it means an ongoing project that runs continuously without ending, not just one-time initiatives, as security doesn't end at deployment.

FR-07: Process of Patches: Systematic patch management aligns with the MOVEit attack's vulnerability-exploitation pattern, in which a zero-day vulnerability in production software enabled widespread attacks. Chidukwani et al. [4] have identified a capability gap in SME environments regarding patch management process components:

- Vulnerability scanning of production systems every week
- Risk-based patch prioritization (Critical: 48 hours, High: 7 days, Medium: 30 days)
- Patch testing before production deployment
- Emergency patching procedure for a zero-day vulnerability

Implementation: A Patch Management Procedure describes roles, timeframes, and escalation processes. The PMO is responsible for tracking portfolio patch compliance.

FR-08: Vendor Security Monitoring: Continuous security monitoring of vendors is a mechanism to counter threats in the supply chain network that arise after vendor assessments. This part implements the threat intelligence integration advice outlined in Sun et al. [33], monitoring activities:

- Quarterly vendor security review (certification currency, incident history)
- Vendor-related threat intelligence monitoring for vulnerabilities
- Annual Vendor Re-Assessments for HIGH-risk dependencies
- Incident Notification and Response Coordination

Implementation: The Vendor Management Matrix Schedule is kept by PMO. An alert for critical vendors initiates an immediate evaluation.

5.3.4. Group 4: PMO-Level Governance

PMO-level governance elements promote portfolio-level visibility and accountability, which address a major problem: fragmented controls that allowed both the HSE and MOVEit incidents to occur.

FR-09: Portfolio Security Dashboard: Centralised security situational awareness for all active projects eliminates the problem of security risks becoming invisible to management, preventing HSE's High Risk status from going unnoticed for long periods. Dashboard metrics (which are not limited to the following):

- Security Classification Distribution of Project (High/Medium/Low)
- Security Gate Performance Levels
- Outstanding Security Findings by Severity Level
- Patch Compliances Status
- Vendor Risk Exposure Summary

Implementation: The dashboard is updated weekly via automated data gathering, if possible; otherwise, via manual reporting. The executives assess this information monthly.

Tool Requirement: Basic dashboard functionality (spreadsheet-based will be sufficient in smaller organizations, but a dedicated GRC tool in larger SMEs).

FR-10: Secured Security Budget: Budget allocation for security, with the possibility of reallocation by senior management, can address the resource-prioritization shortcomings identified in the case studies. PwC noted in 2021 that security expenditure lost out in budget competition without being guaranteed [39] budget components:

- Project security overhead is calculated based on the risk level
- Funding for projects related to standing security
- Security training allocation
- Emergency remediation reserve (10% contingency

Protection Mechanism: The reallocation of the security budget must include a written risk acceptance at the executive level. PMO escalates budget pressure to the governance board.

FR-11: Security Governance Board: Regular governance reviews help ensure that security risks are addressed at the appropriate executive level and that resource allocation decisions are formally recorded.

The meeting structure includes a monthly PMO security review focused on operational aspects, complemented by a quarterly executive security briefing addressing strategic concerns, and additional ad hoc reviews for critical issues as needed. The agenda typically covers a summary of the portfolio's overall security posture, updates on high-risk projects, recommendations for resource allocation, and any proposed changes to security policies and procedures.

FR-12: Security Incident Response Integration: Extensive incident response procedures are followed when responding to security incidents. This is because the incident response was chaotic, according to the HSE case analysis integration components:

- Incident categorization and escalation procedure

- Communication protocols (internal and external)
- Process for post-incident review and lessons learned
- Integration with project security runbooks (FR-05)

Implementation: The Security Incident Response Procedure identifies responsibility, communication paths, and recovery order.

5.4. Implementation Guidance

5.4.1. Phased Implementation Approach

Framework implementation takes on a three-step plan calibrated to the SME change management capability (Table 3):

Table 3: Recommended framework implementation approach

Task Description	Duration
Phase 1: Foundation	Months 1–3
Establish the PMO security governance role.	
Implement risk classification (FR-01) for new projects.	
Create portfolio security dashboard (FR-09)	
Define protected security budget (FR-10)	
Phase 2: Integration	Months 4–6
Deploy security gates (FR-02 to FR-05) for HIGH-risk projects	
Implement Agile security integration (FR-06) for iterative teams.	
Establish patch management process (FR-07)	
Implement vendor monitoring (FR-08)	
Phase 3: Optimisation	Months 7–9
Extend security gates to MEDIUM-risk projects.	
Establish Security Governance Board (FR-11)	
Refine incident response integration (FR-12)	
Continuous improvement based on metrics analysis	

Nine months is the benchmark for organisations with less change management capability. More mature organisations or those with set resources may condense phases, while organisations facing greater resistance may stretch them. The critical factor is the phase order, not the duration.

5.4.2. Role Responsibilities

A clear role definition provides the accountability gaps that were identified in the case analysis (Table 4):

Table 4: Role and responsibilities

Role	Primary Responsibilities
PMO Security Lead	Framework oversight, dashboard maintenance, governance coordination
Project Manager	Gate compliance, security requirements, vendor assessment
Scrum Master	Sprint security integration, security story prioritisation
Technical Lead	Security architecture review, testing coordination
Functional/Business Manager	Risk acceptance for business-owned systems, user access approvals, and security awareness within the department
Executive Sponsor	Budget protection, governance participation, risk acceptance

Counterfactual Conclusion: Although the framework could not protect against zero-day attacks in third-party software, monitoring (FR-08) and effective patch management (FR-07) would have enabled a quicker incident response.

5.4.3. Success Metrics

Measurement of Framework effectiveness enables continuous improvement; hence, it is necessary to keep monitoring by specifying the monitoring metrics. The performance of project security can be evaluated using both leading and lagging

indicators. Leading indicators provide proactive insight into security readiness and include metrics such as maintaining a security gate compliance rate above 95%, reducing the average time from risk identification to mitigation, ensuring a high security story completion rate in Agile projects, achieving patch compliance targets (100% for critical and over 95% for high-severity issues), and completing security awareness training for more than 90% of stakeholders. In contrast, lagging indicators assess outcomes after implementation, including the number of security incidents linked to project deliverables, the cost of post-deployment vulnerability remediation, audit findings related to project security, and the mean time to detect (MTTD) vulnerabilities. Together, these indicators provide a comprehensive view of both preventive effectiveness and actual security performance.

5.5. Framework Validation: Counterfactual Analysis

HSE Ireland Case: Framework Application: This analyzes the framework application for the HSE Ireland case (Table 5).

Table 5: Risk governance and remediation strategy

Failure Point	Framework Component	Prevention Mechanism
Cybersecurity has been rated "High Risk" for 2+ years without action	FR-01 + FR-10	HIGH classification triggers mandatory security requirements; protected budget prevents reprioritisation
No network segmentation despite known risk	FR-04 + FR-10	The security architecture review mandates network segmentation and remediation of protected budget funds.
No centralised security oversight	FR-09 + FR-11	Portfolio Dashboard provides visibility; Governance Board ensures accountability.
Uncoordinated incident response	FR-12	Documented incident response procedures enable a coordinated response

Framework implementation would have forced the organisation to respond to the known HIGH-risk status within the 3-month Phase 1 implementation window, rather than allowing the condition to persist for over 2 years.

5.5.1. MOVEit Case: Framework Application

This analyzes the framework application for the MOVEit case (Table 6).

Table 6: Risk mitigation and framework mapping table

Failure Point	Framework Component	Prevention Mechanism
Third-party software vulnerability exploited.	FR-02 + FR-08	Vendor assessment identifies critical dependencies; continuous monitoring detects emerging vulnerabilities.
Supply chain risk materialised.	FR-07 + FR-08	Patch management prioritises critical vendor updates; vendor monitoring tracks threat intelligence.
No visibility into downstream impact	FR-09	Portfolio Dashboard tracks vendor exposure across projects

While the framework cannot prevent zero-day vulnerabilities in third-party software, vendor monitoring (FR-08) and rapid patch management (FR-07) would have enabled faster detection and response, potentially reducing impact.

5.6. Framework Development Summary

This paper introduced the framework, called PMO-Led Cybersecurity Integration, that consists of twelve pieces, categorized into four groups based on functionality, which are Waterfall security integration, consisting of five components related to project gates, Agile security integration involving one component that is based on sprints, and two involving continuous monitoring, and lastly, four belonging to PMO governance. The Framework has three unique contributions. Firstly, the Framework addresses the gap between enterprise security frameworks and the resource constraints faced by SMEs. Secondly, the Framework incorporates both the Waterfall and Agile methodologies. This acknowledges the fact that a mix of the two is used in the SME. Lastly, the Framework incorporates forcing functions to address the governance failures documented in the breaches. Counterfactual analysis against HSE Ireland incidents and MOVEit cases shows that framework elements directly

interact with failure symptom patterns. The criteria that allowed both incidents to happen, such as invisible risk, unfunded security, and lack of governance, would have raised alarms within the framework's governance structure.

6. Discussion and Critical Analysis

Critique 1: Three-tier classification systems may not be appropriate for complex investment portfolios. HIGH/MEDIUM/LOW may not offer sufficient detail to projects of varying types.

Rationale: This three-tier classification system balances the resource capability of SMEs; it would become unnecessarily complicated if a more detailed classification system were implemented. However, in the case of a micro-SME with one person playing several roles, this structure itself can become quite burdensome [19]. Also, the time involved will scale within the tier system (for example, the HIGH vendor evaluation will take 4-8 hours compared to the MEDIUM vendor evaluation, which will take 2-4 hours).

Critique 2: Self-assessment of project managers suffers from a conflict of interest. Project managers motivated to complete the project quickly might choose to underclassify to reduce security overhead.

Justification: PMO validation within 48 hours for all classifications, with required PMO Manager sign-off for HIGH risk, offers oversight. Dashboard visibility (FR-09) enables portfolio-based pattern identification; systematic under-classification would be detectable. The framework cannot prevent gaming, but makes gaming detectable and accountable. However, evidence shows that schedule pressures lead to optimism bias in self-assessments, a risk that PMO validation can only partially mitigate [4].

6.1. Critique for Vendor Security Assessment (FR-02)

Critique 1: Initial assessment may not accurately reflect the vendor's ongoing security posture. Vendor security can be compromised post-signing.

Rationale: The above concern is addressed by FR-08 Vendor Security Monitoring. Baseline is established by initial assessment. Ongoing changes are tracked by constant monitoring. The annual review for HIGH-risk vendors is complete.

Critique 2: Vendor assessment takes 4-8 hours, potentially delaying procurement. Assessment time could force the team to bypass or expedite the process.

Rationale: The 4-8-hour assessment rating is for HIGH-risk suppliers who need a full assessment. MEDIUM-risk suppliers need 2-4 hours, while LOW-risk suppliers may need minimal assessment. This is to avoid MOVEit-type incidents in which weaknesses in the vendor are exploited by attackers and spread to millions of clients. This is made mandatory by the framework.

6.2. Critique for Security Architecture Review (FR-04)

Critique 1: An architecture review may require security expertise that SMEs may not possess. There may be a lack of knowledge about network segmentation or encryption design.

Rationale: The Architecture Security Checklist is a systematic evaluation tool for spotting obvious weaknesses by people without special security knowledge. For projects classified as HIGH risk, third-party security audits are recommended (hire a security consultant).

Critique 2: The review cycle may need more than 4-6 hours for complicated architectures. Complex or large systems will necessitate more detailed consideration.

Rationale: Time estimates reflect the typical SME project scope. Complex systems of architecture (e.g., enterprise integration, cloud deployment) could involve an in-depth review, but enable flexibility through this framework to establish a baseline level of expectation.

6.3. Critique for Security Testing and Validation (FR-05)

Critique 1: Scanning for vulnerabilities can never discover all vulnerabilities. Automated scanning may overlook logic errors, business logic attacks, and zero days.

Rationale: The framework considers scanning a baseline, not a full assurance measure. Penetration testing for HIGH-risk projects identifies flaws in logic. Zero-day issues also arise due to limitations in pre-deployment testing. The standing projects (FR-07, FR-08) within this framework offer continuous detection. However, some gaps in detection are inevitable, as no test environment can detect all vulnerabilities.

Critique 2: How the testing process validates point-in-time security. The test environment may not accurately reproduce the production environment.

Rationale: Justification is valid because it is addressed by production validation in deployment. The FR-05 deliverable security run book includes a production verification list. Schedule of review after deployment includes production verification.

6.4. Critique for Sprint Security Integration (FR-06)

Critique 1: Literature-based rather than case-validated FR-06 has emerged from the DevSecOps literature. Neither HSE nor MOVEit was directly linked with failures on an Agile project.

Rationale: This is a significant limitation. It has been found that, for success in Agile security, team maturity is required; teams unaware of security issues can't manage basic allocation. Agile security has theoretical backing, but practical success has yet to be established. It needs t be tested by pilot implementations in future work.

Critique 2: The CI/CD pipeline assumption may not hold for all SMEs. SMEs without the necessary DevOps infrastructure may lack the capability for automated security scanning.

Rationale: This framework requires that teams without CI/CD infrastructure implement manual security checkpoints at equivalent points. Tool recommendations include free/open-source tools that will benefit resource-constrained teams. FR-06 varies from fully automatic to manual checkpoint process implementations. The framework's flexibility can handle varying levels of maturity, but its effectiveness declines when no automation is involved.

6.5. Critique for Patch Management (FR-07)

Critique 1: SLA for critical patches is too optimistic at 48–72 hours. Key personnel may be unavailable, testing may be required, and there may be multiple maintenance windows, all of which can constrain rapid patching.

Rationale: The SLA targets are security-appropriate because critical flaws with active exploitation can be exploited within hours. The extension authority mechanism is a structured escalation for genuine constraints: Technical Lead within 12 hours, PMO Manager within 24 hours, and Executive in rare cases. Extensions must be justified in writing to prevent habitual delays while maintaining flexibility. The chronic extensions indicate that patching capacity is the bottleneck, and researchers require investment in infrastructure, not process adjustments.

Critique 2: SMEs might not have patching infrastructure to deploy faster. Organizations without automated tools face a significant challenge in manually patching hundreds of systems.

Rationale: Framework does not require any specific tooling. Monthly cycles for non-critical patches accommodate manual processes. Critical patch escalations ensure that resources are mobilized when required. Investment in patch management tooling is accounted for as an infrastructure improvement, funded from a protected security budget.

6.6. Portfolio Security Dashboard (FR -09)

Critique 1: Dashboards can create a false sense of security-a green status may indicate that security is under control even when unknown vulnerabilities exist.

Rationale: Dashboard metrics reflect process compliance and known risk levels; they do not assure the absence of unknown vulnerabilities. This limitation is acknowledged in the framework. The effectiveness of a dashboard depends on complementary detective controls, scanning and monitoring, and consistent data capture. Users must understand that these dashboards assist decision-making but do not ensure user security.

Critique 2: Dashboard metrics might count activity and not outcomes. Conformity metrics, like the % of gates completed, are not indicative of actual security improvement.

Rationale: This is a fair concern about any metrics-guided governance. The framework contains outcome indicators-vulnerability counts and patch compliance-to provide balance to process indicators. Breach prevention, as the ultimate metric, is hard to attribute, although counterfactual analysis offers theoretical validation.

6.7. Secured Security Budget (FR-10)

Critique 1: Determined executives can still find ways around a protected budget. Governance override lets reallocation occur despite the protection.

Rationale: Governance practices cannot compel commitment to the organization. Cybersecurity is viewed by SME leadership as merely an expense, not an investment [27]. This framework creates additional friction, requiring documented acceptance of risk. In the absence of cultural security values, the friction generates paperwork rather than protection.

Critique 2: Budget protection assumes security costs are predictable. Emergency response, zero-day remediation, and incident investigation may exceed plans.

Rationale: A 10% contingency reserve addresses unpredictability. Major incidents may still exceed reserves, but without protected funding, the chronic underfunding seen in studies would persist.

6.8. Framework Boundary Condition

The framework may be ineffective in the certain circumstances: Micro-SMEs with less than 10 employees, where role differentiation is absent in heavily regulated sectors that require prescriptive compliance, in conflict with the need for risk-appropriate flexibility; in organisations with no PMO maturity, with establishment as a prerequisite; in organisations with negative security culture, with the governance process resulting in a theatre of compliance as opposed to security protection.

In this paper, an analysis of the PMO-Led Cybersecurity Integration Framework, addressing sixteen potential criticisms, has been undertaken. These issues that are appearing as a theme within this current analysis include issues of tension with respect to security stringent measures and resource limitations, whereby said issues appear to be resolved through a level of proportionality with regards to risks, issues of limitations with respect to imposing a framework for purposes of promoting a change within an organizational culture, whereby said limitations appear to be resolved through accountability with respect to security deprioritization, and finally, a discrepancy with respect to an appropriate level of practice, whereby an aforementioned discrepancy appears to be resolved through practical, SME-appropriate implementation templates and phased adoption guidance. This framework does not claim to remove security risks. Rather, this framework presents systematic governance actions to address certain failure types—invisible risk, unfunded security, and fragmented accountability—in a way that can be practically implemented, given usual SMEs restrictions. Critical analysis enhances contributions to this field by providing a visible assessment, allowing practitioners to apply with thorough knowledge.

7. Conclusion and Future Work

This paper concludes by presenting an overview of the research findings, assessing the objectives, and proposing directions for further research. The research aims to fill a gap identified in the literature, where no methodology-specific, actionable framework could be found that facilitates integration of cybersecurity by SMEs into their project management practices. Through a literature review and case study, this research has elaborated a PMO-Led Cybersecurity Integration Framework comprising 12 key areas, divided into 4 categories, validated against recorded instances of cyber breaches. The researchers focused on integrating cybersecurity into project management for small and medium enterprises. SMEs account for more than 99% of organisations in the EU, forming the backbone of global economies, yet they remain disproportionately vulnerable to cyber threats. The systematic literature review identified five major findings which formed the basis of this framework. These include: the persistent SME resource constraints that limit cybersecurity capabilities of SMEs, the lack of alignment between PMO Governance structures and cybersecurity requirements, the current challenges in Waterfall Project management methodologies, the trade-off between speed and security that Agile designs face, the SME realities that have inconsistencies with current enterprise frameworks such as NIST CSF, and ISO 27001.

Real-world examples of validation come from the HSE Ireland ransomware case and the MOVEit supply chain breach. Three recurring project management failure patterns emerged: invisible risk – security problems are recognized but ignored (HSE has had a High Risk designation for over two years without any effort to solve); unfunded security – the needs of business functionality for features are prioritized over security spending; and ownership is ambiguous, so high-risk issues remain unresolved. This has had a severe impact, as HSE Ireland has incurred losses of more than €100 million and has taken 4 months to recover. In contrast, in the MOVEit supply chain breach, more than 2,700 organizations and 93 million individuals are

affected globally. In response, the PMO-Led Cybersecurity Integration Framework has been developed on the principles of design science. This framework is divided into twelve sections, categorized in four sets: Waterfall Security Integration (FR-01 to FR-05) applies security gates at the start, planning, design, and implementation phases; Agile Security Integration (FR-06) integrates security into agile planning events and CI/CD pipelines; Standing Security Projects (FR-07 to FR-08) maintains security on a constant watch using a systematic patching process and security monitoring of suppliers; and PMO Governance (FR-09 to FR-12) offers portfolio-level visibility with security dashboards, secured security budgets, governance boards, and streamlined incident response. All five objectives were accomplished:

- The systematic literature review found cybersecurity issues specific to SMEs for both predictive and adaptive project management approaches.
- Objective 2 was accomplished through case study analysis, extracting recurring failure patterns from documented breaches.
- A framework of twelve elements was constructed that applies to both the waterfall and Agile approaches.
- Counterfactual validation confirmed that applying this framework would have remedied the governance failures that led to the breaches.
- The paper includes templates for security gates, vendor reviews, and Agile security integration.

The research provides both theoretical and practical aspects. Theoretical aspects include filling the gap in PMO security by emphasizing using the PMO as a catalyst for overall security integration rather than treating security as a separate task for IT. It provides a framework applicable regardless of the methods used, including Hybrid approaches, as seen in SME organisations. This paper also presents a risk-proportionate governance model based on a three-tier classification (HIGH/MEDIUM/LOW) that accounts for both stringent security requirements and resource constraints. Practical applications include a framework that provides elements ready for immediate application, complete with time estimates, and an approach that requires a 9-month rollout. However, there are some limitations. This research relies solely on secondary sources, with no direct validation from SME practitioners. The model is validated counterfactually rather than in real time. The Agile aspect of the security integration piece (FR-06) is based on DevSecOps research, not on case studies, as none of the cases focused on failures related to Agile. These are some limitations, but they indicate areas for further research rather than proving ineffective at closing a knowledge gap.

7.1. Recommendations for Future Work

Although the above study offers a validated conceptual framework, the extent of its practicality and development remains to be fully explored. The future efforts must be divided among the following five top priorities:

- **Empirical Validation and Agile-Specific Analysis:** After performing counterfactual validation, an empirical pilot study should be conducted to document issues encountered during implementation, as well as adoption and security outcomes. Concurrently, a case study should be conducted to embed FR-06 based on failures similar to those in the research, validating Waterfall components, using breach incidents at HSE and MOVEit.
- **Adaptation for AI and New Threats:** It should adjust and provide more guidance on AI's dual nature as both an attack mechanism and a defensive tool. Research should be conducted to improve risk classification (FR-01) and testing (FR-05) for AI-aided threats, and to identify ways AI tools can mitigate the limitations posed by SMEs, such as initial AI-based risk assessment and intelligent patches.
- **Scalability and Maturity Modelling:** This framework will assume that the PMO structure applies in resource-constrained SME environments. The maturity model needs to account for how this evolves in an ever-expanding company that employs a dedicated security team. It would then provide an opportunity for SMEs to assess their maturity and implement a roadmap that scales as complexity evolves.
- **Industry-Specific Customization:** General templates must be adapted for high-risk industries. The high-risk industries that should be prioritised for adaptation include healthcare (NHS DSPT and HIPAA regulations), finance (PCI-DSS and FCA regulations), and manufacturing (convergence of OT/IT security).
- **Mechanisms for Continuous Evolution:** To remain effective in this context of dynamically changing threats, mechanisms such as built-in currency systems would be required. Future research would focus on developing mechanisms such as annual threat intelligence updates (e.g., ENISA and DBIR), alignment updates (e.g., NIST CSF 2.0), and others.

In conclusion, Cybersecurity integration into the management of SMES in projects is no longer optional; it is a business imperative. This is the case because the complexity of cyber-attacks, combined with regulatory pressure and supply chain dependence, requires SMEs to incorporate security into how they run their projects. Further, this study proves that the governance failures that lead to key breaches, namely the lack of risk visibility, unfunded security, and lack of accountability,

can be remediated systematically by the PMO in the integration of security. There is no intention in the framework to remove security risks, but rather to offer systematic governance approaches that make security visible, funded, and accountable throughout project delivery.

Acknowledgement: The author gratefully acknowledges the academic support and research environment provided by Northumbria University, which played a vital role in the completion of this study.

Data Availability Statement: Data utilized in this study can be made available by the author upon reasonable request, in line with applicable guidelines.

Funding Statement: No external funding or financial support was received for this research.

Conflicts of Interest Statement: The author confirms that there are no competing interests associated with this work.

Ethics and Consent Statement: Ethical principles were upheld throughout the study, and informed consent was obtained from all participants.

References

1. S. Afaneh, M. R. Al-Mousa, H. S. Al-Hamid, B. S. Al-Awasa, M. Alia, H. Almimi, and A. A. Alkhatib, "Security Challenges Review in Agile and DevOps Practices," in *2023 International Conference on Information Technology (ICIT)*, Amman, Jordan, 2023.
2. S. Al-Janabi, H. Jabbar, and F. Syms, "Cybersecurity Transformation: Cyber-Resilient IT Project Management Framework," *Digital*, vol. 4, no. 4, pp. 866–897, 2024.
3. R. Budiman, T. Raharjo, and A. Suhanto, "Scrum Project Management Challenges and Solutions: Systematic Literature Review," in *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED)*, Sukabumi, Indonesia, 2022.
4. A. Chidukwani, S. Zander, and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," *IEEE Access*, vol. 10, no. 8, pp. 85701–85719, 2022.
5. CISA and FBI, "StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability," *CISA and FBI*, 2023. [Accessed by 12/04/2025].
6. Cyber Ireland, "Conti Cyber Attack on the HSE," *Independent Post Incident Review*, 2021. [Accessed by 18/04/2025].
7. A. Drechsler and A. Hevner, "Knowledge Paths in Design Science Research," *Foundations and Trends in Information Systems*, vol. 6, no. 3, pp. 171–243, 2022.
8. A. Emer, M. Unterhofer, and E. Rauch, "A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises," *IEEE Engineering Management Review*, vol. 49, no. 2, pp. 98–109, 2021.
9. ENISA, "ENISA Threat Landscape 2025," *ENISA*, 2025. [Accessed by 22/01/2026].
10. GitLab, "What Is Agile DevSecOps?" *GitLab*, 2024. [Accessed by 28/04/2025].
11. G. Goldkuhl, "Design Science Epistemology: A Pragmatist Inquiry," *Scandinavian Journal of Information Systems*, vol. 32, no. 1, pp. 39–80, 2020.
12. L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating Cost–Benefit Analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," *Journal of Cybersecurity*, vol. 6, no. 1, pp. 1–8, 2020.
13. M. H. Harake, "Integrating Cybersecurity into Project Management: Best Practices, Emerging Trends, and Strategic Approaches," *PM World Journal*, vol. 14, no. 1, pp. 1–38, 2025.
14. S. Hussain, H. Anwaar, K. Sultan, U. Mahmud, S. Farooqui, T. Karamat, and I. K. Toure, "Mitigating Software Vulnerabilities through Secure Software Development with a Policy-Driven Waterfall Model," *Journal of Engineering*, vol. 2024, no. 1, pp. 1–15, 2024.
15. R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic Literature Review on Security Risks and Its Practices in Secure Software Development," *IEEE Access*, vol. 10, no. 1, pp. 5456–5481, 2022.
16. W. Kim, S. Kim, and H. Lim, "Malicious Data Frame Injection Attack without Seizing Association in IEEE 802.11 Wireless LANs," *IEEE Access*, vol. 9, no. 1, pp. 16649–16660, 2021.
17. F. Lange and I. Kunz, "Evolution of Secure Development Lifecycles and Maturity Models in the Context of Hosted Solutions," *Journal of Software: Evolution and Process*, vol. 36, no. 12, pp. 1–50, 2024.
18. U.S. Department of Defense, "DoD Enterprise DevSecOps Fundamentals," *U.S. Department of Defense*, 2024. [Accessed by 11/04/2025].
19. A. Lindkvist, E. Hoglund, and F. Djebbar, "Cybersecurity Practices, Challenges and Posture in Small and Medium Enterprises: A Survey-Study in Sweden," in *Proceedings of the 24th European Conference on Cyber Warfare and Security*, vol. 24, no. 1, pp. 838–847, 2025.

20. J. Müller, S. Würth, T. Schäffer, and C. Leyh, "Toward a Framework for Determining Methods of Evaluation in Design Science Research," in *Proc. 19th Conf. Comput. Sci. Intell. Syst. (FedCSIS)*, Belgrade, Serbia, 2024.
21. N. Naik, P. Jenkins, P. Grace, D. Naik, S. Prajapat, and J. Song, "A Comparative Analysis of Threat Modelling Methods: STRIDE, DREAD, VAST, PASTA, OCTAVE, and LINDDUN," in *Proc. Int. Conf. Comput., Commun., Cybersecurity and AI (C3AI)*, London, United Kingdom, 2024.
22. NIST, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," *NIST Publication*, Gaithersburg, Maryland, United States of America, 2022.
23. N. M. Nyapete and J. M. Kimani, "Information Security Risk Management in Small Business Enterprises (SMEs)," *African Multidisciplinary Journal of Research*, vol. 1, no. 1, pp. 504–534, 2025.
24. O. M. Oluoha, A. Odeshina, O. Reis, F. Okpeke, V. Attipoe, and O. H. Orieno, "Project Management Innovations for Strengthening Cybersecurity Compliance across Complex Enterprises," *International Journal of Multidisciplinary Research and Growth Evaluation*, vol. 2, no. 1, pp. 871–881, 2021.
25. PCI Security Standards Council, "PCI Security Standards Council Publishes Version 1.1 of Secure Software Lifecycle (SLC) Standard and Program," *Press Release*, 2021. [Accessed by 05/04/2025].
26. R. B. Sulaiman, V. Schetinin, and P. Sant, "Review of Machine Learning Approach on Credit Card Fraud Detection," *Human-Centric Intelligent Systems*, vol. 2, no. 1–2, pp. 55–68, 2022.
27. N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "Perspective of Small and Medium Enterprise (SME's) and Their Relationship with Government in Overcoming Cybersecurity Challenges and Barriers in Wales," *International Journal of Information Management Data Insights*, vol. 3, no. 2, pp. 1–16, 2023.
28. R. B. Sulaiman and A. Khraisat, "Metaheuristic-Driven Feature Selection with SVM and KNN for Robust DDoS Attack Detection: A Comparative Study," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 4, pp. 182–203, 2025.
29. R. B. Sulaiman, A. Kruti, and U. Butt, "A Review of SolarWinds Attack on Orion Platform Using Persistent Threat Agents and Techniques for Gaining Unauthorized Access," *arXiv preprint*, 2023. [Accessed by 19/04/2025].
30. A. Sharma and R. K. Bawa, "Identification and Integration of Security Activities for Secure Agile Development," *International Journal of Information Technology*, vol. 14, no. 3, pp. 1117–1130, 2022.
31. O. Shokunbi, O. Uche, D. Akinwunmi, H. Akinwumi, O. Awodele, and F. Ayankoya, "Security Integration in Agile Methodology," *presented at the 2024 IEEE SmartBlock4Africa*, Accra, Ghana, 2024.
32. A. Sukumar, H. A. Mahdiraji, and V. Jafari-Sadeghi, "Cyber Risk Assessment in Small and Medium-Sized Enterprises: A Multilevel Decision-Making Approach for Small E-Tailors," *Risk Analysis*, vol. 43, no. 10, pp. 2082–2098, 2023.
33. N. Sun, M. Ding, J. Jiang, W. Xu, X. Mo, Y. Tai, and J. Zhang, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1748–1774, 2023.
34. Y. M. Tashtoush, D. A. Darweesh, G. Husari, O. A. Darwish, Y. Darwish, L. B. Issa, and H. I. Ashqar, "Agile Approaches for Cybersecurity Systems, IoT and Intelligent Transportation," *IEEE Access*, vol. 10, no. 12, pp. 1360–1375, 2022.
35. S. T. Kotagiri, "Exploring quantum cryptography for next-generation cybersecurity protocols," *AVE Trends in Intelligent Computer Letters*, vol. 1, no. 1, pp. 21–30, 2025.
36. Y. Valdés-Rodríguez, J. Hochstetter-Diez, M. Diéguez-Rebolledo, A. Bustamante-Mora, and R. Cadena-Martínez, "Analysis of Strategies for the Integration of Security Practices in Agile Software Development: A Sustainable SME Approach," *IEEE Access*, vol. 12, no. 3, pp. 35204–35230, 2024.
37. A. R. P. Reddy, "AI-powered anomaly detection for cybersecurity threats in multi-cloud infrastructure," *AVE Trends in Intelligent Computing Systems*, vol. 2, no. 2, pp. 77–86, 2025.
38. J. Venable, J. Pries-Heje, and R. Baskerville, "FEDS: A Framework for Evaluation in Design Science Research," *European Journal of Information Systems*, vol. 25, no. 1, pp. 77–89, 2016.
39. J. Vom Brocke, A. Hevner, and A. Maedche, "Introduction to Design Science Research," in Design Science Research. Cases, J. vom Brocke, A. Hevner, and A. Maedche, Eds. *Springer International Publishing*, Cham, Switzerland, 2020.