Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 5 | May 2026 -Peer-Reviewed Journal

EFFECTIVE METHODS FOR MANAGING INFORMATION SECURITY PROJECTS

A'zamjonov Abrorbek Erkinjon ugli
Master's Student, Graduate School of Business and Entrepreneurship

ABSTRACT

In the context of rapid digital transformation and increasing cyber threats, effective management of information security projects has become a critical priority for the banking sector. This study examines the applicability of international project management methodologies – PMBOK, PRINCE2, and agile approaches – in managing banking information security projects. Through a comparative theoretical analysis, the research identifies the strengths and limitations of each methodology in relation to the specific characteristics of cybersecurity projects, including high uncertainty, dynamic risk environments, and strict regulatory requirements. The findings reveal that classical methodologies ensure strong governance, structured planning, and compliance, while agile approaches provide flexibility, rapid response, and continuous improvement. However, none of these methodologies alone is sufficient to address the complex and multidimensional nature of banking information security projects. Based on this analysis, the study proposes a hybrid project management model that integrates systematic planning and risk management, institutional governance and control, and agile adaptability. The proposed model enhances the effectiveness of information security management by balancing regulatory requirements with operational agility and supports the development of a resilient and adaptive cybersecurity framework in commercial banks.

KEYWORDS: *Information security, banking sector, project management, PMBOK, PRINCE2, Agile, hybrid model, cybersecurity, risk management, digital transformation*

INTRODUCTION

In the third decade of the 21st century, the global economy has entered a new stage of digital transformation, and the financial services market is undergoing profound structural changes. According to international analyses, the global digital payments market exceeded USD 11 trillion in 2024, while the number of users of mobile financial services approached 3.5 billion. At the same time, according to IBM reports, the average cost of data breaches in 2024 reached USD 4.88 million, with the financial sector remaining one of the most affected industries by cyberattacks.

According to international experts, the number of cyberattacks targeting financial institutions has increased by 2.5 times over the past five years. For banks, the risks are not limited to data loss but also include service disruptions, reputational damage, and economic losses amounting to billions of dollars. As a result, ensuring information security has evolved from a purely technical task to a strategic management priority within the global banking system.

In the Republic of Uzbekistan, large-scale reforms are also being implemented to digitalize the banking and financial system. In recent years, the number of users of remote banking services has increased significantly, and the volume of transactions carried out through mobile banking applications has become dominant in the overall structure of banking operations. According to data from the Central Bank of Uzbekistan, the number of bank cards in circulation has exceeded 50 million, and the volume of cashless payments continues to grow at a rapid pace. However, alongside the expansion of digital infrastructure, cybersecurity threats have also intensified. In 2024, approximately 60,000 cyber threats and 119 major cybersecurity incidents were recorded in Uzbekistan, with the financial sector identified as one of the most vulnerable areas. The economic damage caused by cybercrime exceeded UZS 1.9 trillion. These developments highlight the necessity of adopting new approaches to information security management in the banking sector.

THEORETICAL LITERATURE REVIEW

The growing complexity of cyber threats and the rapid digital transformation of the financial sector have significantly increased the importance of effective information security (IS) project management in banking institutions. Contemporary academic literature emphasizes that IS management is no longer a purely technical function but a strategic governance issue that requires integration with organizational processes, risk management

frameworks, and project management methodologies. In this context, the selection and adaptation of appropriate project management approaches have become a critical research focus.

Classical project management methodologies, particularly PMBOK developed by the Project Management Institute, have been widely recognized in the literature for their structured and process-oriented approach. PMBOK provides a comprehensive framework covering project initiation, planning, execution, monitoring, and closure, with a strong emphasis on documentation and risk management. Scholars argue that this methodology is particularly suitable for large-scale and infrastructure-intensive IS projects due to its systematic planning and well-defined control mechanisms. However, its relatively rigid structure has been criticized for lacking flexibility in dynamic environments, especially in cybersecurity contexts where threats evolve rapidly.

Another prominent methodology discussed in the literature is PRINCE2, developed under the initiative of HM Government. PRINCE2 is characterized by its strong governance orientation, clear allocation of roles and responsibilities, and stage-based decision-making processes. Academic studies highlight its effectiveness in ensuring accountability and maintaining project discipline, particularly in highly regulated sectors such as banking. At the same time, researchers note that the extensive documentation requirements and multi-level approval processes inherent in PRINCE2 may slow down decision-making in situations that require immediate responses to emerging cyber threats.

In contrast to classical approaches, agile project management methodologies, including Agile, Scrum, and Kanban, have gained increasing attention in recent years. The literature emphasizes their adaptability, iterative development cycles, and focus on rapid delivery of results. These methodologies are particularly relevant for IS projects that require continuous monitoring, quick response to vulnerabilities, and incremental improvements. Agile approaches facilitate close collaboration among stakeholders and allow for dynamic reprioritization of tasks in response to evolving threats. However, scholars also identify several limitations, including insufficient documentation, potential challenges in meeting regulatory compliance requirements, and the risk of weakening long-term strategic planning.

Given the limitations of both classical and agile methodologies, recent academic discourse increasingly supports the development of hybrid project management models. Such models aim to combine the strengths of structured approaches (e.g., PMBOK and PRINCE2) with the flexibility of agile methodologies. The literature suggests that hybrid models are particularly effective in complex and high-risk environments, such as banking information security, where both strict regulatory compliance and rapid adaptability are required. These models typically integrate systematic planning and risk management, strong governance and control mechanisms, and iterative improvement processes.

Based on this theoretical foundation, it can be concluded that no single project management methodology is sufficient to address the multifaceted nature of banking information security projects. Instead, a hybrid approach that balances structure and flexibility provides a more effective solution. This perspective underpins the proposed model in this research, which integrates systematic planning, institutional control, and agile adaptability as three core methodological pillars for managing information security projects in the banking sector.

ANALYSIS AND DISCUSSION

The effective management of information security projects in the banking sector is not limited solely to the selection of technical protection tools or compliance with regulatory requirements. The complexity, multi-stage nature, high level of risk, the multiplicity of stakeholders, and the need to implement such projects in parallel with ongoing operational activities necessitate the rational use of modern project management methodologies. Therefore, reassessing and adapting international project management methodologies from the perspective of banking information security constitutes one of the theoretical foundations of this research.

Among the most widely adopted project management methodologies in global practice are the following:

- **PMBOK (Project Management Body of Knowledge)** — a structured and process-oriented approach;
- **PRINCE2** — a methodology focused on governance and control;
- **Agile** — a flexible and iterative management approach;
- **Scrum** — a short-cycle, results-oriented framework;
- **Kanban** — an approach aimed at optimizing workflow;
- **Hybrid methodologies** — integration of classical and agile approaches.

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 5 | May 2026 -Peer-Reviewed Journal

Each of these methodologies possesses specific advantages and limitations when applied to information security projects. Therefore, their comparative analysis is of significant scientific and practical importance.

One of the most fundamental approaches in project management is the PMBOK framework developed by the Project Management Institute. This methodology proposes a systematic approach to project management through the stages of initiation, planning, execution, monitoring, and closure. The primary strengths of PMBOK lie in its structural rigor, strong emphasis on documentation, and well-developed risk management mechanisms.

From the perspective of banking information security projects, the advantages of PMBOK can be summarized as follows: First, the clear definition of project objectives, timelines, resources, and deliverables enables strategic planning of security initiatives; Second, the presence of a dedicated risk management framework aligns well with the nature of information security projects; Third, stakeholder management mechanisms facilitate coordination across multiple departments within banks; Fourth, cost management systems enable effective monitoring of investments in security initiatives.

However, PMBOK also has certain limitations. Due to its relatively rigid and sequential structure, it may lack sufficient flexibility in the rapidly evolving landscape of cyber threats. For instance, if a new threat vector emerges after project initiation, revising the pre-approved plan and budget can be complex. Therefore, while PMBOK is suitable for large-scale infrastructure security projects in banks, it requires adaptation for more agile and responsive security initiatives.

Table 1. ***Advantages and limitations of the PMBOK methodology for banking information security projects***

Criteria	Advantage	Limitation
Planning	High accuracy	Low flexibility
Risk management	Strong	Slow adaptation to dynamic threats
Documentation	High	Increased bureaucratic burden
Cost control	Effective	Difficult to reallocate quickly
Stakeholder management	Strong	Slower decision-making

Thus, PMBOK can be considered an effective methodology for managing banking information security projects in terms of structure and control. However, to align with the rapidly changing nature of modern cyber threats, it should be enhanced with elements of flexible management approaches.

Another widely used methodology in international project management practice is PRINCE2 (Projects IN Controlled Environments). This approach was originally developed under the initiative of HM Government to systematically manage public sector and large-scale institutional projects. Today, it is widely applied in banking, insurance, telecommunications, and major infrastructure projects. The core idea of PRINCE2 is to implement projects under strict governance, with clearly defined roles and responsibilities, and through a stage-by-stage decision-making process.

The PRINCE2 methodology is structured around seven core principles, seven governance themes, and seven processes, providing a comprehensive framework for managing projects under strict control from initiation to completion. Its attractiveness for banking information security projects is primarily обусловлена its strong institutional governance, clearly defined roles and responsibilities, and the presence of stage-by-stage control points throughout the project lifecycle.

In the banking sector, information security projects are typically implemented with the involvement of multiple stakeholders. These include senior management, IT departments, information security units, internal audit, risk management divisions, compliance services, and external technology partners. From this perspective, the PRINCE2 principle of clearly defined roles and responsibilities holds significant practical value for banking information security projects, ensuring effective coordination and accountability across organizational units.

One of the key strengths of this methodology is its mechanism for continuous evaluation of the business justification of a project. PRINCE2 requires that at each stage the question be addressed: “Does the project remain economically and strategically viable?” This approach is particularly important for banking information security projects, as investments in security often do not generate direct financial returns. Therefore, the economic justification of such projects should be reassessed based on factors such as risk reduction, service continuity, and avoided losses.

A second major advantage is the stage-based management approach combined with interim control mechanisms. PRINCE2 divides projects into manageable stages, and at the end of each stage, outcomes are evaluated before proceeding further. In banking information security projects, this approach allows for the structured implementation of complex initiatives, such as:

- establishing a security operations center (SOC);
- strengthening user identification and authentication systems;
- segmenting internal networks;
- implementing continuous monitoring systems.

A third important feature is the controlled change management system. In banking information security projects, evolving cyber threats, emerging regulatory requirements, and technological advancements may alter the project scope. PRINCE2 ensures that such changes are not implemented chaotically but are managed through a formalized and approved governance process. This maintains discipline while preserving a degree of adaptability.

However, the methodology also has certain limitations when applied to banking information security projects. First, the extensive documentation requirements. PRINCE2 necessitates a large number of management documents, reports, and approval stages, which may lead to delays in environments where rapid response to cyber threats is critical.

Second, its relatively low level of agility. Due to its reliance on structured governance processes, decision-making may be slower in rapidly evolving security environments.

Third, it may be less suitable for operational-level rapid security initiatives. For example, implementing immediate countermeasures against emerging fraud schemes may be hindered by the additional bureaucratic layers inherent in PRINCE2 processes.

Table 2. ***Advantages and limitations of the PRINCE2 methodology for banking information security projects***

Criteria	Advantage	Limitation
Governance control	Very strong	Slower decision-making
Allocation of responsibilities	Clearly defined	Requires multi-stage approvals
Stage-based implementation	Effective	Slower in rapid-response projects
Economic justification	High	Evaluation process is complex
Change management	Structured	Relatively low flexibility
Documentation	Systematic	Increased administrative burden

Based on the above analysis, it can be concluded that PRINCE2 represents an effective methodology for managing banking information security projects, particularly in large-scale and strategic initiatives such as infrastructure modernization, the establishment of centralized security management systems, and the development of business continuity centers. However, in projects requiring rapid response and dealing with dynamic threats, its rigid governance structure may lack sufficient flexibility.

Therefore, in managing information security projects in the banking sector, achieving a balance between strong governance control and adaptability becomes a critical methodological issue.

The rapidly evolving nature of threats in the field of information security, the increasing sophistication of cyberattack tools, the continuous discovery of new vulnerabilities, and the expansion of digital banking services have elevated the importance of flexible management approaches alongside traditional, structured methodologies. Many information security initiatives in banks require short-term results, rapid adaptation, and iterative improvement rather than rigid long-term planning. From this perspective, agile project management approaches have gained significant scientific and practical relevance in managing banking information security projects.

The central idea of agile management lies in viewing a project not as a fully predefined and rigid process, but as a dynamic system that evolves through continuous reassessment, short-term deliverables, and adaptation to changing conditions. In this approach, projects are divided into smaller stages, and at the end of each stage, results are evaluated to determine subsequent actions. This model closely aligns with the nature of information security projects in the banking sector.

The first key advantage of agile management is its high level of adaptability. Cyber threats in banking are not static; they evolve continuously. For instance, threats targeting user account compromise may quickly shift toward large-scale attacks on payment systems. In such an environment, rigid long-term planning becomes ineffective, whereas agile approaches allow for rapid reprioritization in response to emerging threats.

The second advantage is the ability to deliver results in short cycles. In banking security projects, it is often more effective to enhance security incrementally rather than attempting full-scale system modernization at once. For example, initiatives such as:

- Implementing two-factor authentication systems;
- Segmenting internal networks;
- Upgrading transaction monitoring systems;
- Introducing security awareness training programs for employees can be successfully implemented through short iterative cycles.

The third advantage is close stakeholder collaboration. In banking institutions, security is not solely a technical issue. Risk management, internal audit, operational services, legal departments, and customer service units all play a role in shaping security decisions. Agile approaches ensure continuous stakeholder involvement, thereby improving the practicality and effectiveness of decision-making.

However, agile approaches also present certain limitations in the context of banking information security projects. First, the relatively low level of documentation. Given that the banking sector operates under strict regulatory oversight, all decisions, security changes, and control mechanisms must be thoroughly documented. Agile methodologies, which emphasize practical outcomes over documentation, may create challenges from a compliance and audit perspective. Second, the potential weakening of long-term strategic vision. Continuous focus on short-term tasks may lead to insufficient attention to the development of a comprehensive security architecture. Third, the potential reduction in centralized governance. In the banking sector, certain security decisions must be made under strict central control. Agile approaches, with their emphasis on flexibility and speed, may sometimes weaken centralized oversight.

Table 3. ***Advantages and limitations of agile project management approaches for banking information security projects***

Criteria	Advantage	Limitation
Flexibility	Very high	Long-term planning may weaken
Rapid results	High	Systematic approach may weaken
Stakeholder involvement	Active	Decision-making may become prolonged
Innovative solutions	Facilitated	Difficulties in documenting regulatory compliance
Rapid response	Effective	Control mechanisms may weaken

Thus, agile project management approaches demonstrate high effectiveness in banking information security projects, particularly in the following areas:

- Rapid response to emerging threats;
- Timely mitigation of vulnerabilities;
- Step-by-step improvement of internal processes;
- Development of employee security awareness;
- Rapid adaptation of digital services from a security perspective.

However, considering the strict regulatory environment of the banking sector, audit requirements, and the need for strategic security governance, relying solely on agile approaches is insufficient. Therefore, the integration of control-oriented classical methodologies with flexible management approaches appears to be the most optimal solution.

The comparative analysis of international project management methodologies discussed above indicates that relying on a single methodology is not sufficiently effective for managing information security projects in the banking sector. This is primarily due to the complex and multidimensional nature of such projects. On the one hand, these projects require rigorous planning, regulatory compliance, documentation, and strong governance mechanisms; on the other hand, the dynamic nature of cyber threats, the rapid pace of technological change, and the continuous evolution of risk factors necessitate a high degree of adaptability in management.

Therefore, the development of a hybrid management model, based on the integration of classical and agile approaches, emerges as the most appropriate scientific and practical solution for managing banking information security projects.

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2026): 8.748 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 13 | Issue: 5 | May 2026 -Peer-Reviewed Journal

According to the author, an effective model for managing information security projects in the banking sector should be built upon three methodological pillars: first, systematic planning and risk management; second, institutional governance and stage-based control; third, rapid adaptability and continuous improvement.

Based on this triad, a hybrid project management model for banks is proposed. The methodological structure of this model is formed as follows:

- The planning and risk management component — based on the PMBOK approach;
- The governance control and allocation of responsibilities component — based on PRINCE2 principles;
- The rapid response and continuous improvement component — based on agile management approaches.

In other words, this model can be expressed through the following formula:

Systematic planning + strong governance control + rapid adaptability = an effective model for managing banking information security projects.

Within this model, the project life cycle is not strictly linear but is organized based on a two-level management architecture.

Table 4. ***Components of the proposed hybrid model***

Management Element	Core Approach	Function in Banking IS Projects
Strategic planning	Systematic approach	Defining objectives and resources
Risk analysis	Systematic approach	Prioritizing risks
Allocation of responsibilities	Control-based approach	Identifying responsibility centers
Stage-by-stage control	Control-based approach	Ensuring project discipline
Rapid adaptability	Agile approach	Responding to emerging threats
Continuous improvement	Agile approach	Enhancing security continuously
Monitoring and evaluation	Integrated approach	Measuring performance

The proposed hybrid model offers several advantages for the banking sector.
First, it establishes a balance between regulatory requirements and operational needs.
Second, it enables more efficient utilization of resources allocated to information security.
Third, it strengthens coordination between bank management and technical units.
Fourth, it provides the ability to respond flexibly to the evolving nature of cyber threats.
Fifth, it transforms information security projects from one-time initiatives into a continuous and evolving management process.

According to the author's scientific conclusion, in order to enhance the effectiveness of information security management in commercial banks of Uzbekistan, it is advisable to implement a hybrid management model based on the integration of classical and agile project management methodologies. This model serves as a theoretical and methodological foundation for further empirical analysis and the development of practical recommendations in subsequent chapters of the dissertation.

CONCLUSION

The theoretical review demonstrates that effective management of information security projects in the banking sector requires a comprehensive and balanced methodological approach. Classical project management frameworks, such as PMBOK and PRINCE2, provide strong foundations in terms of structured planning, governance, documentation, and risk control. These approaches are particularly suitable for large-scale, strategic, and compliance-driven initiatives where stability and accountability are critical. However, their rigidity and procedural complexity limit their effectiveness in rapidly evolving cybersecurity environments.

Conversely, agile methodologies offer significant advantages in terms of flexibility, rapid response, iterative development, and stakeholder collaboration. These characteristics make them highly relevant for addressing dynamic cyber threats and implementing short-term security improvements. Nevertheless, their недостаток in formal documentation, long-term strategic orientation, and centralized control poses challenges in highly regulated banking environments.

Therefore, the analysis confirms that relying on a single methodology is insufficient for managing the complex and multidimensional nature of banking information security projects. Instead, a hybrid project management model that integrates systematic planning and risk management, strong governance and control mechanisms, and agile adaptability emerges as the most effective approach. Such a model enables banks to balance regulatory compliance with operational efficiency, optimize resource utilization, and respond effectively to evolving cyber threats.

REFERENCES (APA STYLE)

1. *IBM. (2024). Cost of a data breach report 2024. https://www.ibm.com/reports/data-breach*
2. *World Bank. (2024). Global digital payments and financial inclusion report. https://www.worldbank.org*
3. *Statista. (2024). Digital payments market size worldwide. https://www.statista.com*
4. *Central Bank of Uzbekistan. (2024). Annual report. https://cbu.uz*
5. *Kaspersky. (2024). Cyberthreat landscape report. https://www.kaspersky.com*
6. *Project Management Institute. (2021). A guide to the project management body of knowledge (PMBOK® Guide) (7th ed.). PMI.*
7. *AXELOS. (2017). Managing successful projects with PRINCE2 (6th ed.). The Stationery Office.*
8. *AXELOS. (2020). Managing successful projects with PRINCE2 (7th ed.). AXELOS.*
9. *Highsmith, J.. (2009). Agile project management: Creating innovative products (2nd ed.). Addison-Wesley.*
10. *Schwaber, K. & Sutherland, J.. (2020). The Scrum guide. Scrum.org.*
11. *Anderson, D. J.. (2010). Kanban: Successful evolutionary change for your technology business. Blue Hole Press.*
12. *ISO. (2022). ISO/IEC 27001: Information security management systems — Requirements. ISO.*
13. *NIST. (2023). Cybersecurity framework (CSF 2.0). NIST.*
14. *IBM. (2024). Cost of a data breach report 2024. IBM Security.*
15. *ENISA. (2023). Threat landscape report.*
16. *World Bank. (2022). Financial sector cybersecurity: Regulatory and supervisory practices.*