Strategic Program Management Models for Secure Ai Adoption in Critical It Infrastructure

[1] Kumar Saurabh
[1] IT Program Management, Project Management Institute, California, USA

Received: 18th Nov 2025 | Received Revised Version: 28th Nov 2025 | Accepted: 28th Dec 2025 | Published: 18th Jan 2026

Volume 08 Issue 01 2025 | Crossref DOI: 10.37547/tajet/Volume08Issue01-12

Abstract

The adoption of artificial intelligence (AI) to critical IT infrastructure offers substantial opportunities for efficiency, resiliency and automation, but also means that you face complex and significant security, governance and operational risks. Traditional project-based implementation approaches are often inadequate for dealing with the long-term, cross-functional and high-risk nature of AI systems in safety-critical and mission-critical environments. This article investigates strategic program management models as an enabling frame for secure and sustainable adoption of Artificial Intelligence (AI) in critical IT infrastructure. It examines the shortcomings associated with ad hoc and siloed AI deployment strategies and makes the case for program level governance structures with integrated security, compliance, risk, and lifecycle oversight. The paper investigates established program management models such as governance-driven, capability based, and hybrid adaptive and assesses their appropriateness for AI initiatives that work in the face of stringent regulatory and cybersecurity constraints. Key enablers such as stakeholder alignment, security-by-design, continuous risk assessment and organizational maturity are discussed in the context of critical infrastructure requirements. The article further suggests a structured program management approach that will bring the AI innovation together with security assurance, regulatory compliance, and operation resilience. By synthesizing the insights from program management theory, cybersecurity governance and from artificial intelligence lifecycle management, this study provides organizations with both a practical framework and strategic foundation to responsibly deploy AI in critical IT environments.

Keywords: Artificial Intelligence Governance, Program Management, Critical IT Infrastructure, Cybersecurity Strategy, Secure AI Adoption.

Cite This Article: Saurabh, K. (2026). Strategic Program Management Models for Secure Ai Adoption in Critical It Infrastructure. The American Journal of Engineering and Technology, 8(01), 87–96. https://doi.org/10.37547/tajet/Volume08Issue01-12

1. Introduction: AI Adoption Challenges in Critical IT Infrastructure

1.1 Background and Context

Critical IT infrastructure supports fundamental services that, when disrupted, will have disastrous implications for national security, economic stability and social well-being. Such infrastructure includes systems supporting energy production and distribution, telecommunications, transportation, healthcare, financial services, and government operations.

These environments are characterised by high availability requirements, long system lifecycles, high regulatory oversight and low tolerance to failure (Djenna et al., 2021; Barbashina, 2023). As the pace of digital transformation quickens, critical infrastructure operators are increasingly turning to advanced information systems to manage complexity, ensure resilience, and respond to evolving operational demands.

Artificial intelligence (AI) has become an important enabler in this regard, offering opportunities for automation, predictive analytics, anomaly detection, and decision support in critical IT environments. AI-driven systems are now being used for optimizing energy grids, increasing the efficiency of cybersecurity monitoring, improving operation efficiency and enabling real-time decision-making in safety-critical environments (Govea et al., 2024; Yigit et al., 2025). This newfound dependence is both a function of technological maturity and of strategic pressure to improve performance and resilience amid unacceptable threats and operational complexity.

However, AI-enabled infrastructure has some fundamental differences from traditional IT systems. Traditional systems tend to be rule-based, deterministic, and relatively static once deployed. In contrast, AI systems are data-driven models that can evolve over time, rely on a continuous stream of data, and exhibit non-deterministic behavior (Schneider et al., 2023). These characteristics create new challenges in governance, security, and accountability, especially when AI components are part of mission-critical environments. As a consequence, the implementation of AI in critical IT infrastructure cannot be considered a regular technology renewal but rather a strategic change with long-term consequences.

1.2 Security and Risk Issues of AI Integration

The integration of AI into critical IT infrastructure greatly increases the method of attack into the system. In addition to the traditional vulnerabilities associated with networks, software and hardware, AI systems offer new risk vectors associated with pipelines to feed data into a machine; how a model is trained; how the model makes inferences; and how the automated decision logic is implemented (Chinnappaiyan, 2025; Yigit et al., 2025). Adversaries can provide attacks during data preparation, manipulating data with poisoning, manipulation during inference time and exploitation during the implementation and monitoring of models, compromising the system integrity and trustworthiness.

Data integrity is a central issue because AI systems are remarkably sensitive to the quality, source, and security of input data. Compromised and biased data can lead to erroneous outputs, unsafe decisions, or even cascading failures across dependent systems (Djenna et al., 2021). Model tinkering and a lack of robustness add to these risks and concerns, especially when it is taken for granted that the outputs of AI models and their algorithms translate into operational control or security measures and responses. Moreover, the limited explainability and transparency of complex AI models make incident analysis, regulatory compliance and accountability difficult, which are key requirements within regulated infrastructure sectors (Schneider et al., 2023; Papagiannidis et al., 2025).

The consequences of AI failure or compromise in critical IT environments could be severe. Malfunctioning or maliciously manipulated AI systems may disrupt vital services, compromise service safety margins, or amplify the impact of cyberattacks (Govea et al., 2024). At a strategic level, such incidents may lead to a loss of public trust, regulatory sanctions and geopolitical and sovereignty-related risks, especially where critical infrastructure is linked to national cybersecurity strategies and digital sovereignty objectives (Barbashina, 2023; Tridgell, 2025). These dangers highlight the need for robust governance and security frameworks that go beyond mere technicalities.

1.3 Shortcomings of Project-Centric AI Implementation

Despite the strategic importance of AI in critical IT infrastructure and its associated risk profile, AI is still adopted by organizations through isolated, project-centric initiatives. Traditional ways of managing projects emphasize adherence to predefined scope, time, and deliverables and often prioritize short-term implementation success over long-term operational assurance (Lycett et al., 2004; Wu et al., 2023). While appropriate for well-bounded IT projects, this approach is not well-suited to the evolving and lifecycle-intensive nature of AI systems.

Project-centric deployment is the cause of what often ends up as fragmented ownership terms between technical development teams, between the cybersecurity function, operational units, and governance bodies. Such fragmentation reduces holistic visibility of risk and accounts for poor accountability of continuous model performance, security posture, and compliance (Pellegrinelli et al., 2007). As AI systems need constant monitoring, re-training, and adaptation to new emerging threats, a lack of sustainable governance mechanisms opens up loopholes to be exploited by adversaries or system failures.

In addition, project-based approaches find it difficult to adapt to changing regulatory mandates and strategic policy changes related to AI governance, cybersecurity, and digital sovereignty (Kshetri, 2024; Monteiro & Singh, 2025). Once a project is formally closed, mechanisms for managing cumulative risk, benefits realization, and cross-system dependencies are often poor. This limitation is especially problematic in critical infrastructure, where the AI capabilities need to be kept secure, compliant, and aligned with the organization's strategy on long-term horizons.

1.4 Research Aim and Structure of Article

In light of these challenges, this article argues for the use of a strategic program management perspective guide to secure AI integration in the domain of critical IT infrastructure needs. Program management provides a governance-oriented framework that is capable of coordinating a number of interrelated initiatives, managing long-term risk, and aligning technology change to strategic objectives (Lycett et al., 2004; Trzeciak et al., 2022). By focusing less on individual projects and more on coordinated programs, organizations will be better able to meet the complexity, uncertainty, and security requirements inherent in AI-enabled critical systems.

The main goal of this article is to discuss the critical role of ensuring secure and resilient adoption of AI for secure and compliant AI adoption in critical IT infrastructure using strategic program management models. It aims to answer the following questions: how do program management principles fit into the AI lifecycle and governance requirements; which program management models work best in high-risk regulated environments; what key enablers do we need for effective implementation?

The remainder of the article is structured as follows. Section 2 examines program management as a strategic framework for secure AI adoption. Section 3 analyzes specific program management models applicable to critical IT environments. Section 4 discusses key enablers and implementation considerations. Section 5 concludes with implications for research and practice in secure AI governance.

2. Program Management as a Strategic Framework for Secure AI Adoption

2.1 Fundamentals of Program Management

Program management is often defined as the integrated management of multiple related projects and activities undertaken to accomplish strategic goals and provide benefits that could not be achieved by separate projects. Unlike project management, which focuses on the delivery of specific outputs within defined constraints of scope, time, and cost, program management focuses on long-term value creation, strategic alignment, interdependencies, and uncertainty management (Lycett et al., 2004; Pellegrinelli et al., 2007). Portfolio management, in contrast, is a much higher-level management function, setting investment priorities and allocating investments across programs and projects without necessarily managing their internal dynamics and execution (Wu et al., 2023).

Some of the core principles of program management are benefits realization, coordinated governance, adaptive planning, mathematical, and sustained stakeholder engagement. These principles have special relevance under conditions of technological complexity, changing requirements and high levels of risk. Program management frameworks acknowledge that outcomes tend to unfold over time and require continual alignment among strategic intention, operational implementation, and organizational capacity (Trzeciak et al., 2022). As such, program management is not confined only to delivery, but also includes oversight of the lifecycle, organizational learning and strategic control.

In the context of advanced digital technologies, program management has increasingly been recognized as a key enabler of digital transformation. Long-term technology efforts can have interdependent systems, with multiple stakeholder groups, and continuously evolving needs due to external influences such as regulation, market conditions, and threat landscapes (Wu et al., 2023). These characteristics are very similar to the conditions under which AI systems operate when deployed in critical IT infrastructure, making program management a better form of governance than traditional project-centric approaches.

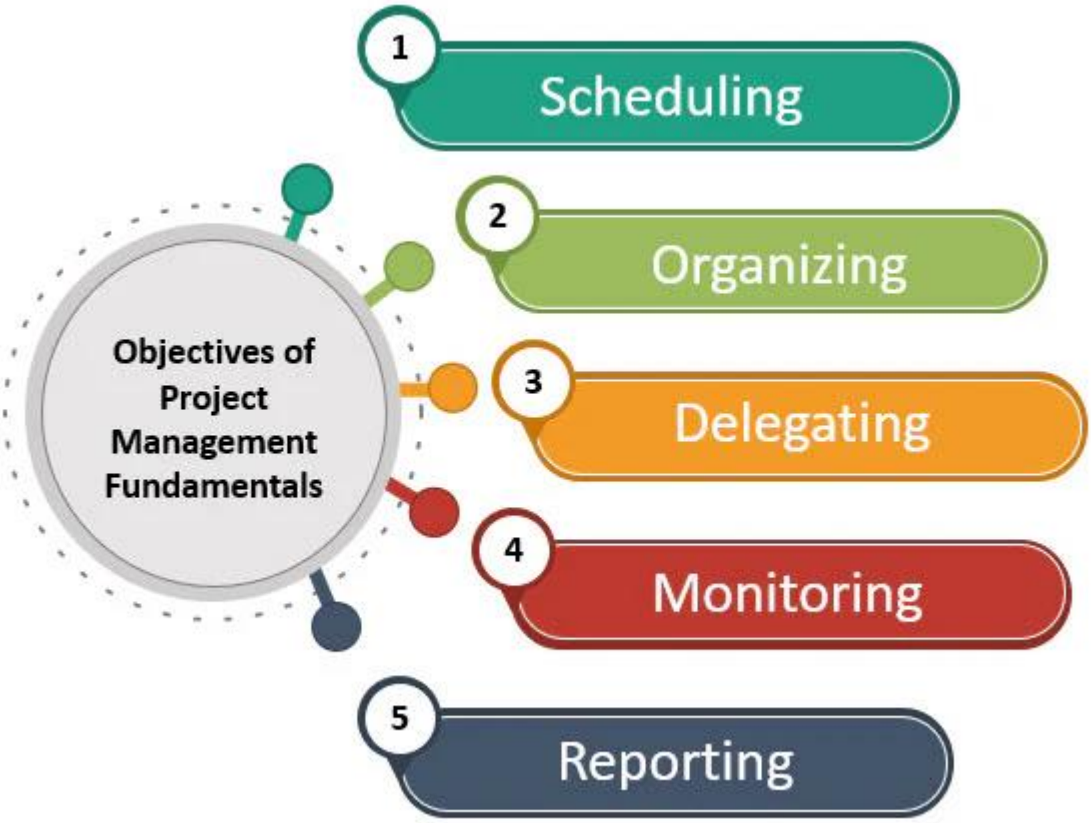

Figure 1: Project Management Fundamentals

2.2 Aligning Program Management with AI Lifecycle Requirements

AI systems have lifecycle properties that fundamentally undermine linear delivery systems. Rather than a one-time build and deploy, AI adoption means evolving cycles of data gathering, model development, model validation, deployment, model evaluations and model retraining. These cycles are further complicated by changing data distributions, varying threats, and evolving operational needs (Schneider et al., 2023; Yigit et al., 2025). Program management is a method of providing a structure for coordinating these ongoing activities under a common strategic vision.

Through a program-based approach, activities of AI lifecycle can be managed as interrelated rather than individual technical activities. This allows the incorporation of security, compliance, and operational oversight into the AI lifecycle and not as post hoc controls. For example, cybersecurity risk management, data governance and regulatory compliance can be engrained as on-going program-level functions that change over time with technical development (Chinnappaiyan, 2025; Papagiannidis et al., 2025). Such integration is essential in critical IT infrastructure, the failure or breach of which might have systemic consequences.

Program management also supports the coordination of complicated interdependencies among sources of data, Artificial Intelligence models, IT infrastructure and organizational stakeholders. AI-enabled critical systems often go across organizational spans, suppliers and regulatory functioning, with dependencies that are impossible to manage in single projects (Pellegrinelli et al., 2007). By keeping an overall perspective about such interconnections, program management helps in proactive risk identification, alignment of resources, and synchronized decision-making across the ecosystem of AI.

2.3 Government and Oversight Mechanisms

Effective governance is a core pillar for program management and a key requirement for secure AI adoption. Program governance structures usually have oversight structures in place, executive sponsorship, and accountability mechanisms defined to guide decision-making processes over long-term time horizons (Lycett et al., 2004). In the context of AI in critical IT infrastructure, such structures are necessary for bringing technical initiatives in line with the organization's strategy, regulatory requirements, and national cybersecurity priorities (Barbashina, 2023).

Program governance boards play a key role in finding ways to balance competing objectives, such as innovation, security, cost efficiency and compliance. They represent a forum for integrating the policies on cybersecurity, data governance, and AI ethics in a coherent governance framework (Schneider et al., 2023; Monteiro and Singh, 2025). Executive sponsorship also helps to ensure that AI programs receive sufficient and sustained strategic attention and that risk-related decisions are escalated to appropriate levels of authority.

Decision-making structures dropping down into programs is a particularly important consideration when it comes to managing the AI risks. Program-level mechanisms facilitate organizations by providing tools to define criteria for accepting risks, establish the escalation route, and respond to new or emerging threats or changes in regulations in a coordinated manner (van Steen, 2025). This is particularly relevant in the case of critical infrastructure, as in these situations, risk tolerance is low, and accountability requirements are high. By incorporating these mechanisms into risk management in program governance, organizations can see a shift from reactive risk management towards an anticipatory and resilient posture.

2.4 Value Creation and Risk Reduction

A strategic program management approach allows organizations to balance the velocity of innovation to security assurance needs. Instead of encasing the development of Artificial Intelligence, program management offers structured flexibility that provides room for experimentation and capability growth within fairly set governance (Trzeciak et al., 2022). This balance is important for critical IT infrastructure operators who want to take advantage of AI's benefits without compromising safety and reliability or infringing on compliance.

Program management is also conducive to scalable and repeatable AI adoption. By understanding and addressing many future deployments through shared standards, reusable components and common governance practices, programs can reduce effort duplication and enable the smart growth of artificial intelligence capabilities across the organization (Wu et al., 2023). This scalability is especially useful in critical infrastructure environments, where it may be necessary to deploy AI-driven applications across multiple systems or domains of operations.

Finally, program-level governance helps to increase organizational trust and accountability. Transparent oversight, clear ownership, and ongoing assurance mechanisms contribute to stakeholder confidence in AI-enabled systems, both internally and externally (Papagiannidis et al., 2025). In sectors where both public trust and regulatory scrutiny are high, for example, critical infrastructure, being able to prove responsible and secure adoption of AI is itself a strategic asset.

3. Strategic Program Management Models Applicable to Secure AI Initiatives

3.1 Governance-Based Program Management Models

Governance-driven program management models have control, compliance and standardization as primary mechanisms for managing complex and high-risk initiatives. These models emphasize well-defined governance structures, formal decision-making processes, and compliance with policies, standards, and regulatory requirements (Lycett et al., 2004). In terms of secure adoption of AI, specific models are particularly relevant in regulated or safety-critical contexts, including national infrastructure, energy systems, and public-sector domains, particularly in IT (Djenna et al., 2021; Barbashina, 2023).

One outstanding feature of autonomy-based designs is the prominent role of oversight bodies and central actors in coordinating program activities. This approach aids consistency in protection from security controls, data governance practices, and compliance reporting across several AI-related initiatives (Pellegrinelli et al., 2007). For AI systems embedded within essential IT infrastructure, this degree of standardization will be needed to address systemic risk and align with national cybersecurity approaches and industry-wide regulations (Barbashina, 2023; Tridgell, 2025).

But there are also limitations to governance-driven models in the AI context. AI development frequently involves trial and error, continuous learning, and adaptation to new data and conditions related to threats. Excessive rigidity in the governance structure can slow innovation, limit the ability to respond to escalating hazards, and hinder the refinement of models after deployment in the field. As such, while governance-driven program management offers strong foundations for security and compliance, it may need additional mechanisms to keep pace with the evolving nature of AI systems.

3.2 Capability-Based and Benefits-Driven Models

Capability-based and benefits-driven program management models shift attention from tight program control to progressively building organizational capabilities and achieving strategic benefits. Rather than AI adoption being delivered as a set of discrete, time-bound deliverables, these models focus on developing sustained competencies in data management, model development, cybersecurity, and governance (Trzeciak et al., 2022). This perspective aligns closely with the long-term nature of AI integration in key IT infrastructure implementations.

Within capability-based models, AI efforts are explicitly tied to strategic outcomes such as operational resilience, enhanced situational awareness and a sufficient security posture. Programs are designed to offer incremental benefits while simultaneously boosting organizational maturity in managing risks and opportunities from AI (Wu et al., 2023). This approach can be useful in critical infrastructure settings, as it enables integrating AI capabilities in a phased manner without exposing systems to sudden or uncontrolled risk.

Managing incremental capability maturity is a major challenge met by these models. As AI systems continue to evolve, organizations need to continually review the readiness of their systems in areas like data governance requirements, cybersecurity practices and regulatory compliance (Kshetri, 2024; Papagiannidis et al., 2025). Program management is the level of coordination and oversight that will be required to integrate technical progress with organizational learning and policy development. However, without adequate governance safeguards, models that are capability-based might have difficulty enforcing consistent security standards across large, evolving AI initiatives, especially in highly regulated environments.

3.3 Adaptive and Hybrid Program Models

Adaptive and hybrid program management models attempt to leverage best practices of governance and capability-based approaches through a mix of flexible delivery methods integrated within structured overarching governance frameworks. These models take into consideration the natural uncertainty that comes with AI performance, data quality, and threat evolution, while maintaining program-level controls that are essential to manage the risk and compliance (Pellegrinelli et al., 2007; Wu et al., 2023).

In secure AI initiatives, adaptive models can be used that involve iterative models and development cycles, ongoing feedback, and deft decision elements. This enables components of AI to be optimized according to experiences of operation and emerging security risks within the scope of the values that govern its operation (Chinnappaiyan 2025; Yigit et al. 2025). Hybrid approaches are especially useful in areas where critical IT infrastructure is important, where both adaptability and assurance are needed.

The main trade-off that is related to adaptive and hybrid models is between flexibility and control. Increased flexibility: Can increase flexibility, responsiveness and innovation, but can add complexity to governance and create challenges for oversight. On the other hand, obsessive control might defeat the, to confront the ability to respond well to evolving AI threats (Schneider et al., 2023). Program management constitutes a central role of those types of tensions as they are meant to constitute boundaries to the allowable operation of adaptive practices with only regard to safety and transparency.

3.4 Model Selection Criteria for Critic IT Infrastructure

Selecting an appropriate program management model for secure AI adoption requires careful consideration of things that are contextual for critical IT infrastructure. Regulatory requirements and compliance obligations are the main determining factors because organizations in regulated areas need to show their compliance with cybersecurity, data protection, and AI governance frameworks (Barbashina, 2023; Tridgell, 2025). Governance driven or hybrid models may be more appropriate in environments where there are strict demands for oversight.

Cybersecurity risk appetite and the current threat environment are also factors when it comes to model selection. In high-risk environments, where AI systems are used in environments that are exposed to sophisticated adversaries or in roles that are mission-critical, it may be necessary to have stronger governance and centralized control in place to ensure resilience and accountability (Djenna et al., 2021; van Steen, 2025). For example, the farther from the immediate risk environment, the greater the emphasis on capability development and adaptive practices might be.

Finally, organizational maturity and resources determine the feasibility of various program management models. Organizations with solid government structures and experienced program management capabilities may be able to implement hybrid models comprising control and flexibility. Less mature organizations may need more prescriptive governance frameworks in order to effectively manage AI risks (Lycett et al., 2004; Wu et al., 2023). The acknowledgement of these contextual variables is critical to aligning the management models of programs with security and resilience objectives of critical IT infrastructure.

Table 1: Strategic Program Management Models for Secure AI Adoption

Program Management Model	Key Focus	Relevance to Secure AI in Critical IT Infrastructure
Governance-Based	Centralized control and compliance	Strong security assurance and regulatory alignment, but limited flexibility
Capability-Based	Incremental capability and maturity	Supports gradual AI adoption, requires complementary governance
Adaptive and Hybrid	Flexibility within structured oversight	Balances innovation, security, and evolving threat conditions

4. Key Enablers and Implementation Considerations for Secure AI Programs

4.1 Security-by-Design and Risk Management Integration

Security-by-design is paramount for the adoption of AI in critical IT infrastructure, where failures or compromises may have systemic effects. Rather than implementing security controls after programs are deployed, cybersecurity and risk assessment should be incorporated into program planning and governance from the start. AI systems introduce additional attack surfaces, including data pipelines, model training, and automated decision logic, making them a necessity for an ongoing, adaptive risk management approach (Djenna et al., 2021; Chinnappaiyan, 2025).

Program management enables ongoing threat modeling and vulnerability management throughout the AI lifecycle, so that risks emerging as systems evolve are detected (Yigit et al., 2025). This approach is conducive to adhering to well-known cybersecurity principles such as zero-trust and defense-in-depth, so AI components can be incorporated into existing layered security architectures rather than as a single innovation in and of themselves (van Steen, 2025).

4.2 Stakeholder Coordination and Organizational Alignment

Secure AI programs rely on proper coordination between IT, cybersecurity, legal, operational, and executive stakeholders. The adoption of AI traverses the boundaries within organizations, and fragmented ownership could negatively affect security and compliance (Pellegrinelli et al., 2007; Wu et al., 2023). Program management facilitates a structured way for these stakeholders to work in a unified way towards common objectives, responsibilities, and risk tolerance levels.

Cross-functional coordination is especially key for the implementation of regulatory and ethical requirements into operating practice. Legal and compliance functions, for example, need to work very closely with technical teams to make sure that compliance and data governance criteria are fulfilling their obligations around AI governance on an ongoing basis (Schneider et al., 2023; Papagiannidis et al., 2025). In parallel, change management and workforce readiness are critical to ensure that personnel have an understanding of AI system behavior, system limitations, and system security responsibilities (van Steen, 2025).

4.3 Metrics, Monitoring, and Assurance Mechanisms

Effective metrics and monitoring are required in order to keep control over AI-enabled critical systems. Program-level key performance indicators (KPIs) deliver visibility in security posture, system performance, and compliance at a point in time (Lycett et al., 2004; Wu et al., 2023). These are indicators to support informed decision-making and early identification of emerging issues.

Given the adaptive nature of AI models, it is important to continuously monitor how the system operates and the quality of the data being used so that any degradation in performance and/or any security anomalies are identified (Yigit et al., 2025). Program management is also supportive of auditability and traceability as it creates consistent documentation and review processes, which are required to support regulatory oversight and organizational accountability (Schneider et al., 2023; Papagiannidis et al., 2025).

4.4 Regulatory and Ethical Considerations

Regulatory and ethical issues are key to securing the adoption of AI in critical IT infrastructure. Organizations need to ensure compliance with the data protection, cybersecurity, and AI governance requirements and their operational resilience (Kshetri, 2024; Monteiro & Singh, 2025). Program management facilitates consistent and integrated compliance activities between different AI programs, minimizing inconsistency and regulation risk.

Transparency, accountability, and explainability are especially important if the AI systems affect decisions that are crucial for safety or security. The embedding of these principles in program governance fosters the trust between key stakeholders, such as regulators, stakeholders, and the public, in the long term. (Schneider et al., 2023; Tridgell, 2025).

Table 2: Key Enablers for Secure AI Programs

Key Enabler	Program-Level Role	Primary Benefit
Security-by-design	Embedded security governance	Reduced systemic and lifecycle risk
Continuous risk assessment	Ongoing oversight and escalation	Early detection of threats and failures
Stakeholder coordination	Cross-functional alignment	Improved accountability and compliance
Metrics and monitoring	Performance and assurance tracking	Sustained trust and regulatory readiness
Regulatory and ethical governance	Policy and compliance integration	Lawful, transparent AI deployment

5. Conclusion: Toward Resilient and Secure AI-Enabled Infrastructure

This article has discussed issues inherent to the adoption of Artificial Intelligence in the context of critical IT infrastructure and has proposed that these challenges cannot be addressed in isolation, project-wise. AI systems introduce new levels of complexity, uncertainty, and risk due to their data-driven, adaptive, and often opaque nature, especially when integrated into environments where reliability, security, and regulatory compliance are of major importance (Djenna et al., 2021; Schneider et al., 2023). The analysis underscores the importance of having a prolonged level of governance, consistent oversight, and ongoing risk management throughout the AI life cycle to secure AI adoption.

Program management has been found to be a strategic framework that is capable of fulfilling these requirements. Through emphasis on the principles of long-term carrying value, interdependency, and adaptive governance, program management is allowed to offer the structural organization required to control AI initiatives from the organizational strategic plan and proficiency in English tolerance (Lycett et al., 2004; Pellegrinelli et al., 2007; Wu et al., 2023). In contrast to traditional project management methodologies, program-based methods help organizations make security, compliance, and operational considerations an ongoing responsibility, rather than a one-time deliverable.

For organizations that manage critical IT infrastructure, the implications are of significant importance. Secure AI adoption is not only about ensuring technical controls, but also about appropriate governance frameworks, cross-functional collaboration, and continuous assurance mechanisms. Program management helps in meeting these needs by allowing uniform execution of cybersecurity principles, meeting regulatory compliance, and incorporating ethical AI practices into multiple initiatives (Chinnappaiyan, 2025; Papagiannidis et al., 2025). This approach creates the ability to increase organizational resiliency whilst enabling controlled innovation in high-risk environments.

From a research and practice perspective, this study is useful by linking program management theory with current AI governance and cybersecurity issues. It underlines the need to see responsible and secure adoption of AI as at least as much an organizational and managerial challenge as a technical one (Kshetri, 2024; Monteiro & Singh, 2025). Future work should focus on refining program management models that can adapt to evolving regulatory landscapes, emerging threat actors, and advancements in AI capabilities to support the secure, scalable, and trustworthy integration of AI into critical IT infrastructure.

References

1. Barbashina (Vorobieva), K. (2023). National Cybersecurity Strategy 2023. Russia and America in the 21st Century, (S3), 0. https://doi.org/10.18254/s207054760029045-6

2. Chinnappaiyan, B. (2025). Navigating AI Security Challenges across Industries: Best Practices for Secure Adoption of Generative and Agentic AI Systems. Journal of Computer Science and Technology Studies, 7(6). Retrieved from https://creativecommons.org/licenses/by/4.0/

3. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences (Switzerland), 11(10). https://doi.org/10.3390/app11104580

4. Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. Systems, 12(5). https://doi.org/10.3390/systems12050165

5. Kshetri, N. (2024, April 1). Economics of Artificial Intelligence Governance. Computer. IEEE Computer Society. https://doi.org/10.1109/MC.2024.3357951

6. Lycett, M., Rassau, A., & Danson, J. (2004). Programme management: A critical review. International Journal of Project Management, 22(4), 289–299. https://doi.org/10.1016/j.ijproman.2003.06.001

7. Monteiro, N., & Singh, V. (2025, December 1). The wheel of artificial intelligence governance. Sustainable Futures. Elsevier Ltd. https://doi.org/10.1016/j.sftr.2025.101279

8. Newswire, P. R. (2024). Building AI Security Confidence: SANS Unveils Toolkit to Guide Secure AI Adoption. PR Newswire US. Y. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib,uid&db=bwh&AN=202410010900PR.NEWS.USPR.UN19710&site=ehost-live&scope=site

9. Papagiannidis, E., Mikalef, P., & Conboy, K. (2025, June 1). Responsible artificial intelligence governance: A review and research framework. Journal of Strategic Information Systems. Elsevier B.V. https://doi.org/10.1016/j.jsis.2024.101885

10. Pellegrinelli, S., Partington, D., Hemingway, C., Mohdzain, Z., & Shah, M. (2007). The importance of context in programme management: An empirical review of programme practices. International Journal of Project Management, 25(1), 41–55. https://doi.org/10.1016/j.ijproman.2006.06.002

11. Schneider, J., Abraham, R., Meske, C., & Vom Brocke, J. (2023). Artificial Intelligence Governance For Businesses. Information Systems Management, 40(3), 229–249. https://doi.org/10.1080/10580530.2022.2085825

12. Tridgell, J. (2025). Open or closing doors? The influence of ‘digital sovereignty’ in the EU’s Cybersecurity Strategy on cybersecurity of open-source software. Computer Law and Security Review, 56. https://doi.org/10.1016/j.clsr.2024.106078

13. Trzeciak, M., Kopec, T. P., & Kwilinski, A. (2022). Constructs of Project Programme Management Supporting Open Innovation at the Strategic Level of the Organisation. Journal of Open Innovation:

Technology, Market, and Complexity, 8(1). https://doi.org/10.3390/joitmc8010058

14. van Steen, T. (2025, March 1). Developing a behavioural cybersecurity strategy: A five-step approach for organisations. Computer Standards and Interfaces. Elsevier B.V. https://doi.org/10.1016/j.csi.2024.103939

15. Wu, X., Klein, G., & Jiang, J. J. (2023). On the Road to Digital Transformation: A Literature Review of IT Program Management. Project Management Journal, 54(4), 409–427. https://doi.org/10.1177/87569728231166846

16. Yigit, Y., Ferrag, M. A., Ghanem, M. C., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., … Janicke, H. (2025). Generative AI and LLMs for Critical Infrastructure Protection: Evaluation Benchmarks, Agentic AI, Challenges, and Opportunities. Sensors, 25(6). https://doi.org/10.3390/s25061666