TRANSFORMING INFORMATION ASSURANCE AND IT SERVICE MANAGEMENT THROUGH DIGITAL ENGINEERING

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Cyber Defense

January 31, 2026

By

John James Darth Vader Bonar

Dissertation Committee:

Patrick Engebretson, PhD

David Kenley, PhD

Matthew Kelso, EdD

The Beacom College of Computer and Cyber Sciences

REVISION HISTORY

Table 1: Revision History of the Dissertaatin

Version	**Date**	**Description of Change**
0.1	2025-OCT-30	Initial draft
0.2	2026-JAN-03	Initial Revision based on Dr. Kenley's feedback
0.3	2026-JAN-21	Minor Revision of Chapter 1 Submitted for Feedback
0.4	2026-JAN-23	Updates to include drafts of Figures, Chapters 2-3, and Appendices
0.5	2026-JAN-31	Initial Draft Submission of Ch. 2 (Ch. 3 and Appendices Removed)

ABSTRACT

Digital Engineering has transformed how the Department of Defense, NASA, and the aerospace industry design, develop, and sustain complex systems. Its four pillars—Model-Based Systems Engineering, digital threads, digital twin, and Product Lifecycle Management—have delivered measurable improvements in mission assurance, configuration management, and lifecycle governance. The Unified Architecture Framework, now codified as ISO/IEC 19540, has emerged as the consolidating standard adopted by major defense organizations and commercial enterprises worldwide. Despite this proven operational value, these methods remain virtually untested within enterprise information technology and information assurance domains. This research investigates whether IT and information assurance professionals recognize the potential that Digital Engineering capabilities hold for their work.

This research targets IT and information assurance professionals across multiple sectors, enabling assessment of whether Digital Engineering awareness and perceived value vary by organizational context. The benefits demonstrated in defense and aerospace suggest logical application to organizations outside these sectors.

The research employs a quantitative survey methodology to collect data across multiple dimensions: awareness, comprehension of specific capabilities, perceived applicability, and value assessments. Systematic literature review documents a near-complete absence of academic research applying Digital Engineering methods to enterprise IT infrastructure or Information Assurance programs. This study establishes baseline empirical data regarding professional awareness and perceived value, furnishing an evidence foundation for strategic decisions regarding future research investment, industry adoption initiatives, and academic curricula development. These results shall inform both scholarly inquiry and practical advancement of mission assurance capabilities.

ACKNOWLEDGMENTS

I extend my profound gratitude to my dissertation committee for their guidance, patience, and insight throughout this journey. Their expertise and steadfast encouragement proved instrumental in bringing this work to fruition.

To my grandparents—Milt and Norma Hoag, Jim and Bertha Bonar—whose legacy of perseverance and principled living continues to inspire me. The values you instilled endure.

To my wife, Sarah, who has been my harbor and my calm through the many years of balancing academic pursuits with professional responsibilities. Your unwavering support made this achievement possible. No words suffice.

To my father, Randy, my mother, Rita, and my brother, Joe. Though I was not always the easiest child to raise, you never wavered in guiding me toward the right path. Your belief in me has been a constant source of strength, and I carry it with me still.

To my cousin, Dr.K̀athryn Fishman-Weaver, whose academic achievements set a standard of excellence and inspired the rest of our family to reach higher. Your accomplishments demonstrated what dedication and intellect can achieve.

Finally, I wish to acknowledge the mentors whose wisdom has shaped my professional journey: Keith Summerson, Dale Kurth, Micah Mogle, Kavi Parupally, Dr.K̀yle Cronin, Dr.C̀asey Mayfield, Kelly Ortberg, Greg Kouski, and Charles Espy Jr. Though years may have passed since our paths crossed, your words of encouragement and guidance continue to resonate.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

When a vulnerability surfaced within federal information systems in late 2023, security teams across multiple agencies found themselves in a desperate race against time. Defenders labored to identify every affected component, racing to understand what adversarial threat actors were already exploiting [1]. Yet they possessed no comprehensive understanding of how vulnerabilities in one system could cascade across interconnected infrastructure and national security systems. Weeks passed while agencies struggled to map the blast radius of potential compromise. During this time adversaries retained the initiative, because existing documentation bore no faithful resemblance to the agencies' actual infrastructure configurations [2]. This operational failure stands not as an isolated incident but as an exemplar of the challenges that modern enterprises confront when managing complex information systems while simultaneously maintaining effective information assurance postures.

The consequences of such failures extend beyond the immediate organizations affected. When defenders cannot comprehend the cascading impacts of compromise, risk communication to organizational leadership degrades, remediation prioritization loses connection to actual impact severity, and defensive coordination across organizational boundaries becomes impractical. The inability to understand system interdependencies transforms what might be contained incidents into enterprise-wide crises. Security teams find themselves engaged in reactive firefighting rather than proactive defense, expending resources on manual discovery efforts that automated, model-based approaches accomplish in minutes rather than weeks.

Information assurance, as codified by the National Institute of Standards and Technology, encompasses those measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation [3]. Cybersecurity constitutes an operational component within this broader discipline, concentrating specifically upon the protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Throughout this dissertation, the term *information assurance* denotes the broader discipline encompassing security policy, risk management, compliance verification, and protective measures. The term *cybersecurity* refers specifically to the technical and operational dimensions of protecting systems from cyber threats. These terms serve distinct purposes and shall not be employed interchangeably: information assurance represents the broader governance and assurance framework, while cybersecurity addresses the specific protective mechanisms and threat responses that operate within that framework.

Terminological precision bears operational consequences. Organizations that conflate information assurance with cybersecurity often underinvest in the governance, documentation, and architectural foundations upon which effective cybersecurity operations depend. The failure to maintain accurate system documentation, for example, represents an information assurance shortfall that manifests as cybersecurity operational degradation. Digital Engineering addresses both dimensions: the governance and documentation requirements of information assurance and the operational visibility requirements of cybersecurity defense.

This chapter examines the challenges organizations encounter when implementing information assurance practices and managing information technology (IT) service delivery, introducing Digital Engineering as a disciplinary approach capable of addressing gaps that persist despite mature frameworks including the National Institute of Standards and

Technology (NIST) Risk Management Framework (RMF) [3], the Information Technology Infrastructure Library (ITIL) [4], and the Unified Architecture Framework (UAF) [5].

1.1 Current State of Information System Management

Organizations today operate within an environment defined by relentless technological evolution and escalating system complexity. The convergence of cloud computing, microservices architectures, Internet of Things (IoT) devices, and operational technology has spawned intricate webs of interdependencies that overwhelm traditional approaches to both information assurance and IT service delivery [6]. These technological advances deliver undeniable operational benefits. But they exact a heavy toll in system visibility, security control implementation, configuration management, and service delivery coordination.

The pace of technological change continues to accelerate. Organizations that required months to deploy new capabilities a decade ago now deploy changes continuously through automated pipelines. This acceleration benefits operational agility but strains the documentation and verification processes upon which information assurance depends. Static documentation approaches designed for quarterly or annual update cycles cannot maintain accuracy when systems change hourly. The structural mismatch between documentation velocity and operational velocity creates systematic failures that compound over time.

Enterprise information systems now routinely span multiple technology domains: cloud-based infrastructure and services, on-premises data centers, edge computing environments, operational technology networks, and mobile and remote access systems. This technological heterogeneity generates persistent challenges in maintaining security visibility, implementing consistent protection mechanisms, and delivering reliable IT services across disparate environments. System dependency tracking operates without confidence; configuration management falters; security control implementation proceeds inconsistently across heterogeneous platforms [7].

The challenge extends beyond mere technical complexity. Organizational structures that evolved to manage discrete technology domains now impede the integrated visibility that modern environments require. Security teams operate separately from IT operations teams, while cloud architects work independently of network engineers. Application developers deploy services without understanding infrastructure dependencies. This organizational fragmentation mirrors and reinforces the technical fragmentation that undermines both information assurance and IT service delivery effectiveness.

1.1.1 Information Assurance Practice

The practice of information assurance has evolved in response to the complexities of modern enterprise environments. The NIST Risk Management Framework provides a structured, disciplined approach for managing security and privacy risk that organizations can apply across diverse information systems [3]. The RMF establishes a lifecycle approach to security through seven iterative steps: prepare, categorize, select, implement, assess, authorize, and monitor. This framework has become foundational for federal agencies and finds increasing adoption among organizations operating national security systems and private enterprises seeking systematic approaches to information assurance.

The RMF represents a significant advancement over earlier compliance-focused approaches that treated security as a point-in-time certification rather than a continuous process. The framework's emphasis upon continuous monitoring and ongoing authorization reflects recognition that security postures change constantly as systems evolve, threats emerge, and organizational requirements shift. Effective implementation of continuous monitoring requires capabilities that most organizations lack: real-time visibility into system configurations, automated assessment of control effectiveness, and dynamic risk calculation based upon current rather than documented system states.

Additional information assurance lifecycle frameworks exist including ISO 31000 [8], the NIST Cybersecurity Framework [9], COBIT [10], etc. These frameworks provide alternative approaches to the RMF. However, they share common challenges in maintaining accurate documentation, ensuring visibility into system states, and coordinating security efforts across organizational boundaries. The approach taken by this research is focused on a NIST focused approach, which reduces complexity by avoiding direct comparison among multiple frameworks while still addressing challenges common to all.

Security control selection represents a key RMF activity. Federal information systems and national security systems typically utilize NIST Special Publication 800-53 Revision 5 as the authoritative catalog of security controls [3]. Organizations operating outside federal requirements may employ alternative frameworks for control selection, including ISO/IEC 27001 [11], the NIST Cybersecurity Framework, or industry-specific standards. The methodology presented in this research focuses upon NIST 800-53 Revision 5 given its applicability to federal and national security contexts, though the underlying principles extend to organizations employing other control frameworks.

The selection of appropriate security controls depends upon accurate understanding of the systems being protected, their operational context, their interconnections with other systems, and their role within the broader enterprise architecture. Control selection that proceeds from inaccurate system understanding produces security postures that address documented rather than actual risk. This disconnect between documentation and reality represents a structural challenge that persists regardless of which control framework an organization employs.

Implementing the RMF effectively presents documented challenges in complex technological environments. Organizations must categorize information systems based upon potential impact, select appropriate security controls from comprehensive catalogs, implement those controls across diverse platforms, assess control effectiveness, obtain authorization decisions, and maintain continuous monitoring throughout the system lifecycle. Each step demands accurate, current information about system configurations, security control implementations, and operational states. Traditional documentation approaches struggle to maintain such information.

The continuous monitoring requirement deserves particular attention because it exposes the limitations of document-centric approaches most directly. Continuous monitoring as envisioned by the RMF requires ongoing awareness of security-relevant system changes, automated assessment of security posture impacts, and timely reporting to authorizing officials. Organizations attempting to implement continuous monitoring through manual processes discover that the labor required exceeds available resources. Organizations attempting to implement continuous monitoring through automation discover that they lack the authoritative system models and configuration baselines that automation requires.

1.1.2 IT Service Management Practice

IT service management (ITSM) has matured through frameworks designed to ensure reliable service delivery across the enterprise. The Information Technology Infrastructure Library provides comprehensive guidance for aligning IT services with business needs through structured processes for service strategy, service design, service transition, service operation, and continual service improvement [4]. ITIL emphasizes configuration management, change management, and service asset management as foundational capabilities upon which effective IT service delivery depends.

The evolution from ITIL Version 3 to ITIL 4 reflects recognition that service management practices must adapt to cloud computing, DevOps practices, and agile delivery models. ITIL 4 introduces the Service Value System concept, emphasizing flexibility and continuous improvement over rigid process compliance. Yet the core dependencies upon accurate configuration information and effective change coordination persist regardless of which ITIL version organizations adopt. The Service Value System cannot create value if the underlying information about services, configurations, and dependencies remains inaccurate or incomplete.

Configuration management within the ITIL framework requires organizations to maintain accurate configuration management databases documenting configuration items, their attributes, and their relationships. Change management processes depend upon accurate configuration information to assess change impacts and coordinate modifications across interconnected systems. Service asset management extends these capabilities to encompass the full lifecycle of IT assets from acquisition through retirement. These interconnected processes provide structure for managing complex IT environments. But they depend upon the accuracy and currency of underlying information—accuracy that organizations consistently fail to achieve.

The relationship between configuration management and change management illustrates the compounding nature of documentation failures. Change management processes assess proposed changes against documented configurations and relationships. When documentation is incomplete, change assessments miss dependencies that exist in operational systems. Changes approved based upon incomplete assessments cause unintended impacts. Those impacts require emergency changes to address. Emergency changes bypass change management processes, further degrading documentation accuracy. This cycle perpetuates itself, progressively undermining both configuration management and change management effectiveness.

1.1.3 Challenges in Current Practice

Traditional documentation approaches and manual tracking methods prove increasingly inadequate for capturing and managing the complexity inherent in modern information systems. Paper-based security documentation, static network diagrams, and periodic compliance assessments fail to reflect the dynamic nature of contemporary enterprise environments. IT service management practices that rely upon manual configuration tracking and change coordination struggle to maintain accuracy and timeliness in environments characterized by continuous deployment and rapid change cycles.

The structural challenge lies not in the quality of frameworks or the dedication of practitioners. The challenge lies in the mismatch between the documentation velocity that manual processes can sustain and the operational velocity that modern enterprise environments demand. No amount of process improvement or additional staffing can close this gap using traditional approaches. The solution requires a paradigm shift from document-centric to model-centric practices—precisely the shift that Digital Engineering provides.

Research documents pervasive failures across both information assurance and IT service management domains. Industry analysts report that eighty percent of Configuration Management Database (CMDB) implementations fail to deliver intended value [12]. Studies find that organizations can monitor only sixty-six percent of their IT environments, leaving thirty-four percent unmonitored [13]. Shadow IT—technology acquired or deployed outside official governance—now represents thirty to forty percent of enterprise IT spending, creating assets invisible to documentation efforts [14]. The mean time to identify security breaches averages 204 days, reflecting the visibility gaps that impair threat detection [15].

These statistics represent not merely organizational shortcomings but systemic limitations of document-centric approaches. Organizations that invest heavily in documentation still experience these failures. Organizations with mature governance processes still discover undocumented systems and unknown dependencies. The consistency of these failures across diverse organizations suggests that the problem lies not in execution but in approach.

These failures share a common pattern: organizations cannot maintain accurate, current documentation of their information systems using traditional approaches. The rate of change in modern IT environments exceeds the capacity of manual documentation processes. Static artifacts become obsolete before completion. Configuration databases diverge from operational reality. Security documentation describes intended states rather than actual implementations. This documentation-reality gap undermines every process that depends upon accurate system information—which includes nearly all information assurance and IT service management activities.

Chapter 2 examines these visibility and documentation failures in depth, synthesizing peer-reviewed research and industry analysis to establish the evidence base for why traditional practices fail. Documentation challenges reflect multiple converging factors: organizational silos fragmenting visibility, complexity exceeding human documentation capacity, manual processes unable to match rates of change, and technical debt accumulating in documentation domains.

1.2 Digital Engineering as Potential Solution

Digital Engineering represents a systematic approach to designing, developing, and managing complex systems through integrated digital models and data-driven processes [16]. Originally forged within the defense and aerospace sectors, Digital Engineering has been formalized through authoritative guidance from organizations including the United States Department of Defense (DoD) [17], the National Aeronautics and Space Administration (NASA) [18], and the International Council on Systems Engineering (INCOSE) [16]. While these foundational practices emerged primarily from physical systems engineering, the underlying principles offer capabilities of documented value for information technology and information assurance domains.

The emergence of Digital Engineering from defense and aerospace contexts carries significance beyond historical interest. These sectors developed Digital Engineering practices to address challenges structurally similar to those confronting enterprise IT and Information Assurance: complex interdependent systems, stringent compliance requirements, mission-critical operations, and the need to maintain comprehensive visibility across extended lifecycles. The solutions that proved effective for managing combat aircraft development and spacecraft missions may prove equally effective for managing enterprise information systems and security postures.

Digital Engineering rests upon four foundational pillars: Model-Based Systems Engineering (MBSE), digital threads (the authoritative traceability that connects system lifecycle artifacts), digital twin technology, and Product Lifecycle Management (PLM). Understanding these pillars provides context for examining how Digital Engineering practices might address the challenges identified in current information assurance and IT service management practice.

The integration among these pillars distinguishes Digital Engineering from isolated tool adoption. Organizations might implement modeling tools without achieving Model-Based Systems Engineering, or deploy digital twin capabilities without establishing digital thread traceability. Digital Engineering's value emerges when these capabilities function together as an integrated approach—precisely the integration that current information assurance and IT service management practices lack.

1.2.1 Model-Based Systems Engineering

Model-Based Systems Engineering represents a paradigm shift from document-centric practices to model-centric approaches for system development and management [19]. Rather than relying primarily upon textual descriptions and static diagrams, MBSE employs formal, executable models that capture system architecture, behavior, requirements, and relationships in structured, machine-readable formats. These models serve as authoritative sources of truth that can be analyzed, simulated, and validated throughout the system lifecycle [20].

The distinction between document-centric and model-centric approaches warrants emphasis. Document-centric approaches produce artifacts—diagrams, specifications, procedures—that describe systems. These artifacts require human interpretation, cannot be automatically validated for consistency, and provide no mechanisms for maintaining currency as systems evolve. Model-centric approaches produce executable representations that can be queried, analyzed, and validated automatically. When models change, dependent artifacts update automatically. When proposed changes are evaluated, models enable impact analysis that documents cannot provide.

Architecture frameworks provide the structural foundation for MBSE implementations. The Unified Architecture Framework, developed by the Object Management Group (OMG), offers a standardized approach to enterprise and systems architecture modeling that supports both defense and commercial applications. UAF defines viewpoints and views that enable architects to represent complex systems from multiple perspectives, including operational, service, personnel, resource, security, and project viewpoints. This multi-viewpoint approach aligns naturally with the needs of organizations managing information systems that must satisfy both information assurance requirements and IT service delivery objectives.

Within the context of information systems, MBSE principles enable organizations to create formal models of their IT infrastructure, security architectures, and service delivery processes. These models capture not merely the static configuration of systems but also the dynamic relationships between components, the flow of information through the enterprise, and the dependencies that affect both security postures and service delivery. Model-based approaches provide enhanced visibility into system complexity, enable automated analysis of security implications for proposed changes, and support more effective planning for IT service delivery requirements. The integration of MBSE with established frameworks such as the NIST RMF and ITIL enables organizations to maintain living models that reflect both security control implementations and service configuration states.

1.2.2 Digital Threads

Digital threads constitute authoritative traceability—the verified, bidirectional connections between requirements, design elements, implementation artifacts, and validation activities that persist throughout a system's lifecycle [21]. The term "digital threads" describes the connective tissue that weaves together authoritative sources including Model-Based Systems Engineering models, requirements management systems, configuration management databases, and Product Lifecycle Management repositories into a unified, navigable fabric of system information. Digital threads ensure that organizations can track how requirements flow through the development and implementation process, identify which system components implement specific capabilities, and verify that implemented solutions satisfy intended requirements. Unlike traditional documentation approaches, digital threads maintain verified relationships that remain current as systems evolve [22].

The concept of authoritative traceability deserves careful attention. Traditional traceability attempts to maintain connections through manual cross-references, requirements matrices, and documentation linkages. These manual traceability mechanisms require constant maintenance, degrade as systems evolve, and provide no automated verification of consistency. Digital threads establish traceability through model relationships that update automatically as models change. Queries against digital thread repositories return current rather than historical information. Impact analyses traverse digital thread connections to identify affected components throughout the system architecture.

For information assurance practice, digital threads address gaps in current RMF implementation. The RMF requires organizations to select security controls, implement those controls, and assess their effectiveness throughout the system lifecycle. Digital threads enable organizations to trace security requirements from categorization decisions through control selection, implementation, and assessment activities—connecting policy documents to technical configurations to assessment evidence in a single authoritative chain. This traceability supports the continuous monitoring phase of the RMF by maintaining verifiable connections between security requirements, implemented controls, and compliance artifacts.

Within IT service management contexts, digital threads align with ITIL configuration management and change management practices. Organizations can trace service delivery requirements to underlying infrastructure components and configuration items, connecting the CMDB to as-built system documentation and operational baselines. This capability supports more accurate impact assessment for changes and more effective root cause analysis for service disruptions. The ability to maintain current, verified traceability relationships through digital threads reduces the time and effort required for compliance audits while improving the accuracy of both security assessments and service impact analyses.

1.2.3 Digital Twin

Digital twin technology creates virtual replicas of physical or logical systems that maintain synchronization with their real-world counterparts through continuous data exchange [23]. These virtual representations enable organizations to simulate system behavior, analyze potential changes, predict future states, and optimize performance without disrupting operational systems [24]. Digital twins combine real-time operational data with analytical models to provide dynamic, predictive capabilities that extend far beyond traditional monitoring and simulation approaches [25].

The synchronization between digital twins and operational systems distinguishes this technology from traditional simulation and modeling approaches. Static models represent intended or designed system states. Digital twins represent current operational states, updated continuously through integration with operational data sources. This synchronization enables digital twins to support operational decision-making in ways that static models cannot: predicting the impact of proposed changes based upon current rather than documented configurations, identifying emerging issues before they cause operational impact, and supporting real-time optimization of system performance.

In information assurance contexts, digital twin capabilities offer advantages for security control validation and risk assessment. Organizations can create digital twins of their information systems to simulate security scenarios, test control effectiveness, and analyze attack vectors in environments isolated from production operations. These virtual representations enable security teams to evaluate the impact of proposed security controls, assess the effectiveness of defensive measures, and predict system behavior under various threat scenarios. Digital twins support RMF assessment activities by enabling organizations to test security configurations and validate control implementations before deployment to production environments.

For IT service delivery, digital twins support capabilities aligned with ITIL service design and service transition practices. Organizations can employ digital twins for capacity planning, change impact analysis, and service optimization by enabling teams to test changes and analyze performance implications before implementing modifications in production environments. The ability to simulate proposed changes in a synchronized virtual environment reduces the risk of service disruptions while supporting more rapid and confident change implementation.

1.2.4 Product Lifecycle Management

Product Lifecycle Management provides frameworks and toolsets for managing information, processes, and resources throughout a system's entire lifecycle from initial conception through retirement [26]. PLM integrates data from diverse sources, maintains configuration baselines, manages change processes, and ensures that stakeholders access current, accurate information about system states and changes. This integrated approach to lifecycle management extends beyond simple version control to encompass configuration management, change coordination, release management, and information governance.

The application of PLM principles to information systems represents a conceptual extension from its origins in manufacturing and product development. Physical products have lifecycles that parallel information system lifecycles in important ways: conception, design, development, deployment, operation, maintenance, and retirement. PLM practices developed for managing physical product lifecycles address challenges—configuration management, change coordination, baseline maintenance—that information system managers confront daily. The question is whether PLM tools and methodologies can be adapted effectively for information system contexts.

Applied to information systems, PLM principles address challenges in managing complex IT infrastructures and security postures throughout the system lifecycle. The RMF explicitly recognizes the importance of lifecycle management, requiring organizations to maintain security controls and documentation throughout system operation and into decommissioning. PLM approaches support these requirements by managing security control baselines, coordinating changes across interconnected systems, maintaining configuration integrity, and ensuring that security teams operate from consistent, current information throughout the authorization boundary.

PLM capabilities align closely with ITIL service lifecycle management concepts. Organizations can implement PLM frameworks to support ITIL configuration management by maintaining authoritative configuration baselines and managing configuration item relationships. PLM change coordination capabilities enhance ITIL change management by providing improved visibility into change impacts across service dependencies. The ability to maintain integrated views of system configurations, security controls, and service delivery components reduces inconsistencies between security and IT operations teams, improves change coordination, and supports more effective compliance management across the system lifecycle.

1.3 Gaps in Current Practice

Despite advances in information assurance methodologies and IT service management frameworks, organizations continue to encounter challenges that limit their effectiveness in protecting information assets and delivering reliable services. The NIST Risk Management Framework and ITIL provide structured approaches to information assurance and IT service management respectively. Yet implementation challenges persist across both domains. Examining these gaps illuminates where Digital Engineering practices might offer valuable enhancements to current practice.

The persistence of these gaps despite framework maturity and organizational investment suggests that the challenges reflect structural limitations rather than implementation failures. Organizations following established frameworks with dedicated resources still experience documentation failures, visibility gaps, and traceability shortfalls. These outcomes indicate that the problem lies not in how organizations execute current approaches but in inherent limitations of document-centric methodologies.

1.3.1 Information Assurance Challenges

Organizations implementing the NIST Risk Management Framework struggle to maintain visibility into their security postures across complex, distributed information systems. The RMF continuous monitoring phase requires organizations to maintain ongoing awareness of security control effectiveness and system security state. Security teams often lack accurate, current understanding of system configurations, security control implementations, and the dependencies that affect security effectiveness. This visibility gap manifests throughout the RMF lifecycle: organizations find it difficult to track security dependencies effectively, leading to unidentified vulnerabilities when changes are implemented. The inability to maintain accurate documentation of system interconnections and data flows, particularly in environments with rapid deployment cycles, impairs the effective risk assessment and incident response capabilities that the RMF demands.

The challenge of understanding cascading impacts deserves particular attention. When security incidents occur or vulnerabilities are discovered, defenders must rapidly assess which systems are affected, what data is at risk, and how compromise of one system might enable access to interconnected systems. This assessment requires understanding of system dependencies that current documentation approaches cannot maintain. The inability to trace first, second, and third order impacts transforms incident response from a precision operation into a broad search effort that consumes time and resources while adversaries retain the initiative.

Security control implementation presents particular challenges in modern enterprise environments characterized by hybrid cloud deployments, distributed architectures, and frequent changes. Organizations must implement and maintain consistent security controls from NIST SP 800-53 across diverse platforms while supporting continuous deployment practices and rapid update cycles [3]. Traditional security configuration management approaches fail to scale effectively in these dynamic environments, leading to inconsistent security postures and compliance gaps. The challenge compounds when organizations attempt to validate control effectiveness across interconnected systems where authorization boundaries grow increasingly complex to define and maintain.

1.3.2 IT Service Management Challenges

IT service management faces parallel challenges in maintaining accurate system documentation. Configuration Management Database implementations fail at documented rates approaching eighty percent, leaving organizations without authoritative sources for configuration information [12]. Manual configuration tracking cannot keep pace with the rate of change in modern IT environments. Shadow IT creates blind spots where undocumented systems introduce unknown dependencies and security risks. Change management processes suffer when impact assessments rely upon incomplete or inaccurate dependency information.

The economic dimensions of these failures warrant examination. Organizations invest considerable resources in CMDB implementations, documentation efforts, and change management processes. When these investments fail to deliver intended value, organizations face difficult choices: invest additional resources attempting to improve failing approaches, accept degraded capabilities and increased risk, or seek alternative approaches that address root causes rather than symptoms. Digital Engineering represents one such alternative approach.

The convergence of these challenges creates a compounding effect where neither information assurance nor IT service management can achieve their objectives independently. Security teams cannot effectively assess risks without accurate understanding of IT infrastructure. IT teams cannot effectively manage changes without understanding security implications. Both domains require the visibility and accurate documentation that current practices demonstrably fail to provide.

1.3.3 The Documentation-Reality Gap

The persistent gap between documentation and operational reality represents the common thread connecting failures across both domains. Security documentation describes control implementations that may not exist as documented. Configuration databases contain information that no longer reflects system states. Network diagrams depict architectures that have evolved beyond their documented form. This gap undermines every process that depends upon accurate system information.

When documentation diverges from reality, security assessments measure fiction rather than fact. Change impact analyses miss dependencies that exist but are not documented. Incident responders waste time discovering that documented configurations do not match operational systems. Compliance auditors cannot verify that documented controls exist in practice. The documentation-reality gap transforms information assurance and IT service management from disciplined practices into exercises in uncertainty.

Digital Engineering addresses this gap through its emphasis upon authoritative sources of truth, continuous synchronization between models and operational systems, and automated verification of consistency between documentation and reality. The question this research investigates is whether IT and information assurance professionals recognize the potential value of these capabilities for their work.

1.4 Research Questions

Based upon the challenges documented in current practice and the potential capabilities offered by Digital Engineering, this research investigates the following questions:

1. To what extent are information technology and information assurance professionals aware of Digital Engineering capabilities, including Model-Based Systems Engineering, digital threads, digital twin technologies, and Product Lifecycle Management principles?

2. Do information technology and information assurance professionals perceive Digital Engineering capabilities as potentially valuable or important for their work in information assurance, security compliance, and IT service delivery?

3. Do information technology and information assurance professionals believe that Digital Engineering practices could help them in performing their jobs, meeting compliance requirements, or enhancing organizational capabilities in information assurance and IT service delivery?

These research questions focus upon professional awareness and perceptions as foundational investigation. Establishing awareness levels and perceived value represents an essential first step before investigating practical implementation approaches, organizational adoption strategies, or empirical validation of Digital Engineering benefits in information assurance and IT service management contexts.

1.5 Research Scope and Approach

This research examines professional perceptions across several key areas. The investigation focuses upon awareness and perceived value of Model-Based Systems Engineering approaches for representing information system architectures and security controls. It examines whether professionals perceive value in digital threads for maintaining authoritative traceability between security requirements, control implementations, and compliance evidence as required by frameworks such as the NIST RMF. The research explores perceptions of digital twin capabilities for security simulation, testing, and IT service modeling. And it investigates whether professionals perceive value in Product Lifecycle Management principles for managing information system configurations and security control baselines throughout the system lifecycle.

1.5.1 Methodological Approach

The research employs a quantitative survey methodology to collect data from IT and information assurance professionals. Survey methodology enables systematic data collection from a broad population of practitioners, supporting statistical analysis and generalization of findings. The anonymous nature of survey research encourages candid responses about professional knowledge gaps and organizational capabilities. Chapter 3 presents the complete research methodology including survey design, sampling strategy, and analytical approach.

The choice of survey methodology reflects considered evaluation of alternative approaches. A case study or implementation pilot would provide rich contextual data about Digital Engineering application in specific organizational settings. However, such approaches cannot establish whether the broader professional community recognizes value in Digital Engineering capabilities or possesses awareness of these methodologies. Professional perceptions represent a necessary foundation for adoption: practitioners will not adopt approaches they do not recognize as valuable, regardless of demonstrated technical merit. Understanding current awareness and perceived value therefore precedes and informs subsequent research into implementation approaches.

1.5.2 Target Population and Broader Application

This research targets IT and information assurance professionals across the broad spectrum of organizations where these practitioners operate. The survey population encompasses professionals working in defense, government, commercial, healthcare, education, and non-profit sectors. This inclusive approach enables assessment of professional perceptions across diverse organizational contexts rather than limiting findings to specific industry sectors.

The target population selection reflects a deliberate methodological choice with implications for how research findings may be applied. By surveying IT and information assurance professionals broadly rather than focusing exclusively upon defense or aerospace practitioners, this research establishes baseline awareness and perception data across the professional community. These findings enable assessment of whether Digital Engineering awareness varies by organizational context and whether perceived value differs across sectors.

The defense and aerospace sectors have demonstrated measurable benefits from Digital Engineering adoption. The Department of Defense Digital Engineering Strategy documents improved mission assurance, reduced development timelines, and enhanced configuration management across programs implementing Digital Engineering practices [27]. NASA reports similar benefits from Model-Based Systems Engineering adoption across its mission portfolio [28]. These demonstrated benefits establish that Digital Engineering delivers value in complex, mission-critical contexts requiring stringent compliance and comprehensive documentation.

The question that motivates this research is whether the benefits demonstrated in defense and aerospace contexts may transfer to other organizational settings. IT and information assurance professionals working outside defense and aerospace confront challenges structurally similar to those that Digital Engineering addresses: complex interdependent systems, compliance requirements demanding comprehensive documentation, and the need to maintain accurate visibility across dynamic environments. If Digital Engineering practices prove transferable, organizations across all sectors might benefit from methodologies originally developed for defense applications.

1.5.3 Potential Benefits for Organizations Serving Underrepresented Populations

The potential transferability of Digital Engineering benefits carries particular significance for organizations serving underrepresented and underserved populations. Healthcare providers serving rural communities, educational institutions in under-resourced districts, social service organizations with limited IT budgets, and non-profit entities addressing community needs all require effective information assurance and IT service delivery capabilities. These organizations face the same documentation challenges, visibility gaps, and compliance burdens as large enterprises, often with fewer resources to address them.

Organizations serving underrepresented populations must frequently demonstrate compliance with regulatory frameworks, security standards, and funding requirements. Healthcare providers must satisfy HIPAA security requirements. Educational institutions must protect student data under FERPA. Social service organizations must safeguard client information while demonstrating accountability to funding agencies. These compliance obligations demand documented evidence of security controls and system configurations—documentation that consumes scarce staff time and organizational resources.

If Digital Engineering practices can reduce the burden of compliance documentation while improving documentation accuracy, organizations with limited resources could redirect staff effort toward direct service provision rather than documentation administration. The automated traceability that digital threads provide could reduce the manual effort required for compliance audits. The model-based documentation that MBSE enables could maintain accuracy through automated synchronization rather than manual updates. The configuration management capabilities that PLM provides could reduce the specialized expertise required to maintain accurate system documentation.

This research does not presume that Digital Engineering benefits will transfer effectively to resource-constrained organizations. The survey population targets IT and information assurance professionals broadly, not exclusively those serving underrepresented populations. However, by establishing baseline awareness and perceived value data across the professional community, this research creates a foundation for subsequent investigation of Digital Engineering applicability in diverse organizational contexts. If professionals perceive value in Digital Engineering capabilities, future research can examine practical implementation approaches suitable for organizations with varying resource levels.

The logical pathway from defense and aerospace demonstration to broader application proceeds through several steps. First, defense and aerospace organizations demonstrate that Digital Engineering delivers measurable benefits for complex systems with stringent compliance requirements. Second, research establishes whether IT and information assurance professionals outside these sectors recognize potential value in Digital Engineering capabilities. Third, if perceived value exists, subsequent research can examine implementation approaches, adaptation requirements, and cost-benefit considerations for organizations in different contexts. This research addresses the second step: determining whether professional awareness and perceived value support continued investigation of Digital Engineering for enterprise IT and information assurance applications.

1.5.4 Why Perceptions Matter

The investigation of professional perceptions warrants explanation given the availability of alternative research approaches. Technology adoption research consistently demonstrates that perceived value influences adoption decisions regardless of actual value. Professionals who do not perceive value in a capability will not advocate for its adoption within their organizations. Establishing whether IT and information assurance professionals recognize potential value in Digital Engineering capabilities therefore addresses a prerequisite question for successful adoption.

Furthermore, perception research enables assessment of awareness gaps that might impede adoption. If professionals are unaware of Digital Engineering capabilities, education and communication initiatives become necessary precursors to adoption efforts. If professionals are aware but do not perceive value, the theoretical premise that Digital Engineering addresses recognized needs requires reconsideration. Understanding the current state of professional awareness and perceptions enables targeted strategies for advancing Digital Engineering adoption in information assurance and IT service management domains.

1.5.5 Contribution of Prior Research

By surveying professionals actively working in these domains, this research identifies whether practitioners recognize connections between their current practices and Digital Engineering capabilities. The findings illuminate whether existing information assurance and IT service delivery frameworks already incorporate concepts analogous to Model-Based Systems Engineering, digital threads, digital twins, or Product Lifecycle Management, or whether these Digital Engineering capabilities represent genuinely novel approaches within information technology contexts. This understanding establishes whether Digital Engineering offers new conceptual frameworks for addressing information assurance and IT service delivery challenges or whether it primarily provides different terminology for existing practices.

This research builds upon the foundational work of Bonar and Hastings, who established an initial reference model demonstrating that compliance verification is enhanced and supported by Digital Engineering practices within the context of information systems [29]. The current research extends this foundation by examining whether the broader professional community recognizes value in the capabilities that the reference model proposes.

1.6 Significance of the Research

This research carries implications across academic, industry, commonwealth, and societal dimensions. Understanding these dimensions of significance contextualizes the contribution this investigation makes to knowledge and practice.

1.6.1 Academic Significance

The academic significance of this research lies in identifying whether IT and information assurance professionals recognize a gap that Digital Engineering addresses. The literature review presented in Chapter 2 documents a near-complete absence of academic research applying Model-Based Systems Engineering, digital threads, digital twins, or Product Lifecycle Management to enterprise IT infrastructure or Information Assurance programs. This research gap exists despite explicit requirements within NIST and ITIL frameworks for enterprise architecture capabilities, documentation accuracy, and traceability that Digital Engineering could provide.

By surveying professionals actively working in these domains, this research identifies whether practitioners recognize connections between their current practices and Digital Engineering capabilities. The findings illuminate whether existing information assurance and IT service delivery frameworks already incorporate concepts analogous to Model-Based Systems Engineering, digital threads, digital twins, or Product Lifecycle Management, or whether these Digital Engineering capabilities represent genuinely novel approaches within information technology contexts. This understanding establishes whether Digital Engineering offers new conceptual frameworks for addressing information assurance and IT service delivery challenges or whether it primarily provides different terminology for existing practices.

1.6.2 Industry Significance

For industry practitioners, this research provides insight into how their peers perceive Digital Engineering capabilities. Organizations considering Digital Engineering adoption can benefit from understanding current awareness levels and perceived value within the professional community. If research reveals widespread recognition of Digital Engineering value, organizations may find receptive audiences for adoption initiatives. If research reveals limited awareness or skepticism, organizations can anticipate the education and change management challenges that adoption would require.

The research also identifies which specific Digital Engineering capabilities professionals perceive as most valuable for their work. This information enables tool vendors, service providers, and standards organizations to focus development and communication efforts on the capabilities that practitioners recognize as addressing their needs. Understanding professional perceptions enables more effective resource allocation across the ecosystem supporting Digital Engineering adoption.

1.6.3 Commonwealth Significance

The commonwealth significance of this research relates to national security and protection of societal infrastructure. Federal information systems and national security systems protect information assets and enable government operations upon which citizens depend.

Organizations operating these systems face the challenges documented throughout this proposal: maintaining accurate documentation, implementing consistent security controls, and verifying compliance across complex technical environments.

Digital threads enhance compliance verification and security assurance for systems serving government and societal functions by providing authoritative traceability—verified connections between security requirements, control implementations, and compliance evidence. Operators of these systems must demonstrate compliance with numerous regulatory frameworks and security standards, often requiring extensive manual effort to collect evidence and prepare for audits. Digital Engineering practices reduce the burden of compliance verification while improving the accuracy and currency of compliance documentation, enabling organizations to redirect resources toward proactive security improvements rather than compliance documentation.

The ability to understand first, second, and third order impacts of security incidents carries particular significance for critical infrastructure protection. When adversaries compromise systems supporting government functions or critical infrastructure, defenders must rapidly assess the scope of compromise and potential cascading effects. Digital Engineering practices provide the visibility and traceability that enable rapid, accurate impact assessment—capabilities that current approaches demonstrably fail to provide.

1.6.4 Societal Significance

Beyond organizations operating national security systems, Digital Engineering capabilities benefit organizations serving communities with limited resources. Healthcare providers, educational institutions, social service organizations, and other entities serving underserved populations face the same information assurance and IT service delivery challenges as large enterprises, often with fewer resources to address them.

Digital threads reduce the time and specialized knowledge required for compliance verification, making it more feasible for smaller organizations to demonstrate regulatory compliance and security effectiveness to funding agencies, oversight bodies, and stakeholders. Many organizations serving underserved populations must comply with privacy regulations, security standards, and funding requirements that demand documented evidence of security controls and compliance measures. Digital Engineering practices reduce the burden of generating and maintaining compliance documentation, enabling organizations to redirect limited staff time and resources toward direct service provision rather than compliance administration.

The potential for Digital Engineering to democratize sophisticated security and documentation capabilities represents a notable societal benefit. Currently, enterprise architecture, authoritative traceability, and model-based documentation remain accessible primarily to large organizations with specialized expertise and dedicated budgets. When Digital Engineering tools and practices are adapted for organizations with limited resources, the resulting improvements in security posture and compliance efficiency benefit the communities these organizations serve.

1.7 Chapter Summary

This chapter has established the context for investigating professional awareness and perceptions of Digital Engineering capabilities within information assurance and IT service management domains. The discussion identified the challenges organizations face in maintaining accurate system documentation, implementing consistent security controls, and delivering reliable IT services using traditional document-centric approaches. Digital Engineering, with its four pillars of Model-Based Systems Engineering, digital threads, digital twin technology, and Product Lifecycle Management, offers capabilities for addressing these identified gaps.

The research questions focus upon measuring professional awareness of Digital Engineering capabilities, assessing whether professionals perceive these capabilities as valuable for their work, and determining whether professionals believe Digital Engineering practices could enhance their effectiveness in meeting compliance requirements and delivering IT services. The significance of this research spans academic contribution through addressing identified literature gaps, industry benefit through informing adoption strategies, commonwealth value through enhancing protection of government systems, and societal benefit through potentially enabling better security capabilities for organizations serving underserved populations.

The research targets IT and information assurance professionals across diverse organizational contexts, enabling assessment of awareness and perceived value across the professional community. While the defense and aerospace sectors have demonstrated Digital Engineering benefits, this research investigates whether professionals in other sectors recognize potential value in these capabilities for their work. The findings will inform whether Digital Engineering methodologies developed for defense applications might benefit organizations across all sectors, including those serving underrepresented populations with limited resources for compliance documentation and security administration.

Chapter 2 presents the systematic literature review examining existing research across Digital Engineering, information assurance, and IT service management domains. The review establishes the theoretical framework for this research while documenting the research gaps that this investigation begins to address. Chapter 2 also examines in detail the evidence for enterprise visibility and documentation failures, synthesizing peer-reviewed research and industry analysis to establish why traditional practices fail to maintain accurate system documentation.

Chapter 2

Literature Review

This chapter examines the current body of knowledge across nine interconnected domains relevant to applying Digital Engineering methodologies to Information Assurance and IT Service Management. Through systematic synthesis of research spanning enterprise architecture frameworks, Digital Engineering foundations, Model-Based Systems Engineering, digital twin technology, compliance frameworks, IT service management practices, and enterprise visibility challenges, this review establishes the theoretical groundwork while documenting a research gap: the near-complete absence of academic research applying proven MBSE and Digital Engineering methodologies to enterprise IT infrastructure, IT Service Management, or Information Assurance programs. The chapter culminates in a theoretical framework positing that Digital Engineering represents a disciplinary approach capable of addressing gaps that have persisted despite decades of framework development and organizational investment.

2.1 Enterprise Architecture Frameworks

Enterprise Architecture (EA) provides the foundational structure for understanding, documenting, and managing complex organizational systems. The evolution of enterprise architecture frameworks from domain-specific military applications toward unified commercial and defense approaches reflects growing recognition that systematic architectural methods transcend organizational boundaries. This section examines the major enterprise architecture frameworks and their convergence through the Unified Architecture Framework.

The importance of enterprise architecture frameworks for this research lies in their explicit recognition that complex systems require structured approaches to documentation, visualization, and management. The challenges that motivated enterprise architecture development—complexity exceeding human comprehension, interdependencies requiring systematic tracking, and stakeholder communication requiring multiple perspectives—parallel the challenges that Digital Engineering addresses. Understanding the enterprise architecture foundation provides context for evaluating how Digital Engineering extends and enhances architectural approaches.

2.1.1 The Unified Architecture Framework

The Unified Architecture Framework represents the most notable evolution in enterprise architecture standardization, now codified as ISO/IEC 19540-1:2022 and ISO/IEC 19540-2:2022 through the Object Management Group [5]. UAF emerged from the Unified Profile for DoDAF and the Ministry of Defence Architecture Framework (MODAF) (UPDM 3.0) with the explicit purpose of consolidating multiple defense architecture frameworks while extending applicability to commercial domains. The specification asserts that ninety percent of concepts and themes captured in military frameworks prove equally applicable in commercial domains [30]. This recognition carries implications for enterprise IT and Information Assurance practitioners who have historically operated outside the systems engineering discipline.

UAF employs a grid-based structure wherein rows represent stakeholder domains—Strategic, Operational, Services, Personnel, and Resources—while columns represent architecture aspects. This structure defines seventy-one view specifications through the UAF Domain Metamodel and UAF Modeling Language [31]. The framework's foundation upon the IDEAS Ontology and implementation through UML/SysML profiles addresses a historical limitation: the disconnect between enterprise architecture and systems engineering tools that plagued earlier frameworks [32]. For organizations seeking to bridge the gap between enterprise IT documentation and rigorous systems engineering practice, UAF provides a standards-based pathway.

The grid structure warrants examination because it illustrates how UAF enables multiple stakeholder perspectives on complex systems. Strategic viewpoints address enterprise goals and capabilities. Operational viewpoints describe how organizations accomplish missions. Service viewpoints define the services that systems provide. Resource viewpoints identify the systems and components that deliver capabilities. Security viewpoints address protection requirements and mechanisms. This multi-viewpoint approach enables different stakeholders to examine systems from their particular concerns while maintaining integration across perspectives through the underlying metamodel.

Comparative research by Bankauskaite evaluated enterprise architecture frameworks using weighted criteria spanning domain support, tool support, modeling language openness, information availability, and researcher prevalence [33]. UAF achieved the highest overall rating of 2.8, surpassing TOGAF at 2.3, DoDAF at 1.9, MODAF at 1.8, NAF at 1.6, and FEAF at 1.2. This comparative analysis demonstrates UAF's emergence as the preferred framework for organizations requiring architecture capabilities across multiple domains.

2.1.1.1 UAF as the Consolidating Standard

The Object Management Group developed UAF explicitly as a consolidating standard to address the proliferation of incompatible architecture frameworks that impeded interoperability across organizations and nations. Understanding why OMG positioned UAF as the consolidating framework and why major defense organizations have adopted it illuminates the framework's significance for enterprise applications.

The consolidation imperative arose from practical interoperability challenges. During coalition military operations, allied nations discovered that their architecture frameworks—DoDAF for the United States, MODAF for the United Kingdom, NAF for NATO, and DNDAF for Canada—employed different metamodels, terminologies, and tooling requirements despite addressing similar architectural concerns [34]. Architecture products created in one framework could not be readily consumed by organizations using other frameworks. This incompatibility hampered the coalition planning and capability development that modern military operations require.

OMG convened representatives from the U.S. Department of Defense, the UK Ministry of Defence, NATO, Canadian armed forces, and Swedish armed forces alongside industry partners and tool vendors to develop a unified approach [35]. The resulting UPDM specification, and its evolution into UAF, consolidated the common concepts across military frameworks while extending applicability to commercial domains. The development process explicitly identified that ninety percent of military framework concepts addressed challenges equally relevant to commercial enterprises [30].

The Department of Defense has incorporated UAF into its architecture guidance, recognizing the framework's alignment with Digital Engineering initiatives [17]. The UK Ministry of Defence maintains alignment between MODAF evolution and UAF development. NATO Architecture Framework Version 4 explicitly endorses the UAF Domain Metamodel as a compliant metamodel, validating UAF's role as a unifying framework for defense interoperability across allied nations [36]. This adoption by major defense organizations establishes UAF as the authoritative approach for defense architecture while the ISO standardization extends that authority to commercial contexts.

The consolidation extends beyond military applications. OMG designed UAF to support commercial and industrial enterprises facing similar architectural challenges: complex systems spanning multiple domains, diverse stakeholder perspectives requiring integration, and compliance requirements demanding comprehensive documentation. The UAF specification explicitly addresses both defense and commercial use cases, with viewpoints and views applicable to enterprise IT, service delivery, and organizational capability management [31].

International standardization through ISO/IEC 19540 further establishes UAF's role as the consolidating framework. ISO adoption provides the framework with international recognition that encourages adoption across national boundaries and industry sectors. Organizations seeking architecture frameworks with international standing increasingly select UAF given its dual status as both OMG and ISO standard.

For enterprise IT and Information Assurance applications, UAF's consolidating role carries significance. Organizations can adopt a framework with proven application in complex defense systems while benefiting from commercial domain extensions. The framework provides structured approaches to documenting systems, relationships, and security requirements that align with both NIST and ITIL expectations. The integration with SysML enables model-based documentation approaches that address the accuracy and currency challenges plaguing traditional enterprise architecture implementations.

2.1.2 Department of Defense Architecture Framework

The Department of Defense Architecture Framework (DoDAF) Version 2.02 established the foundational military architecture approach with eight viewpoints and fifty-two models, supporting key DoD processes including the Joint Capabilities Integration and Development System for capabilities definition, the Defense Acquisition System for program management, and the Planning, Programming, Budgeting, and Execution process for resource allocation [37]. DoDAF 2.0's introduction of the DoDAF Meta Model marked the watershed transition from document-based to data-centric architecture products—a transformation in how defense organizations conceptualize and manage architectural information [38].

The transition from document-based to data-centric approaches deserves emphasis because it represents a conceptual shift that Digital Engineering extends. Earlier DoDAF versions specified products—documents and diagrams—as the primary outputs of architecture development. DoDAF 2.0 shifted emphasis to the underlying data, recognizing that products should be generated from authoritative data stores rather than created as standalone artifacts. This shift aligns with Digital Engineering's emphasis upon authoritative sources of truth from which views and reports are generated as needed.

Analysis by the National Defense Industrial Association's Systems Engineering Division documented limitations in the DoDAF Meta Model's support for systems engineering requirements [34]. The analysis identified semantic disconnects with UML and SysML that subsequently informed UAF development. Research by Hause further examined evaluation criteria for DoDAF meta-model support of systems engineering, identifying specific areas where the framework required enhancement to support integrated systems engineering practices [39]. These limitations drove the evolution toward more capable frameworks.

Despite its limitations, DoDAF established principles that persist in successor frameworks. The emphasis upon multiple viewpoints addressing different stakeholder concerns, the recognition that architecture data should support analysis rather than merely documentation, and the integration of architecture with acquisition and capability development processes all originated with or were significantly advanced by DoDAF. Understanding this heritage provides context for UAF's design decisions and explains why UAF maintains compatibility with DoDAF products and processes.

2.1.3 NATO Architecture Framework

The NATO Architecture Framework (NAF) Version 4 explicitly endorses the UAF Domain Metamodel as a compliant metamodel, validating UAF's role as a unifying framework for defense interoperability across allied nations [36]. NAF evolved through multiple versions to address interoperability requirements spanning NATO member nations, with Version

4 representing alignment with international standardization efforts. The framework supports coalition operations planning and capability development through standardized architectural descriptions that enable communication across organizational and national boundaries.

NAF's endorsement of UAF carries practical implications. NATO member nations developing architectures using UAF can share and integrate those architectures across the alliance. This interoperability enables coalition planning, joint capability development, and coordinated operations that incompatible frameworks impede. The alignment between NAF and UAF demonstrates how consolidating standards enable collaboration that fragmented standards prevent.

For enterprise applications, NAF's endorsement of UAF validates the framework's applicability beyond single-organization contexts. Organizations operating within supply chains, partnership networks, or regulatory ecosystems face interoperability challenges similar to those confronting coalition military operations. A consolidating framework that enables architecture sharing across organizational boundaries provides value beyond internal documentation.

2.1.4 The Open Group Architecture Framework

The Open Group Architecture Framework (TOGAF) provides comprehensive methodology for enterprise architecture development through its Architecture Development Method [40]. A joint white paper between The Open Group and MITRE Corporation established the complementary relationship between TOGAF and DoDAF, observing that TOGAF focuses primarily upon architecting methodology without prescribing architecture description constructs, while DoDAF focuses primarily upon architecture description through defined views without specifying methodology [41]. This complementary relationship informed UAF's design, which synthesizes both description standards from DoDAF heritage and methodological considerations from commercial frameworks.

TOGAF's prominence in commercial enterprise architecture practice makes this complementary relationship significant. Organizations familiar with TOGAF methodology can adopt UAF for architecture description while retaining TOGAF's Architecture Development Method for process guidance. This compatibility reduces adoption barriers for organizations transitioning from commercial to unified frameworks.

The Architecture Development Method's iterative approach aligns with Digital Engineering principles emphasizing continuous refinement over point-in-time documentation. TOGAF recognizes that architecture evolves as organizations change, requiring processes that maintain architecture currency rather than treating architecture as a completed deliverable. This recognition parallels Digital Engineering's emphasis upon living models that maintain synchronization with operational systems.

2.1.5 Zachman Framework

The Zachman Framework for Enterprise Architecture, developed by John Zachman in the 1980s, provides an ontology for organizing architectural artifacts [42]. The framework's six-by-six matrix structure addresses interrogatives—what, how, where, who, when, and why—across perspectives ranging from executive through implementation. While the Zachman Framework provides taxonomic structure, it does not prescribe specific modeling languages or tools, distinguishing it from more prescriptive frameworks like DoDAF and UAF [43].

The Zachman Framework's historical significance lies in establishing the conceptual foundation that subsequent frameworks elaborated. The recognition that different stakeholders require different perspectives on systems, organized by fundamental interrogatives, influenced all subsequent enterprise architecture development. Understanding this foundation illuminates why modern frameworks like UAF employ multi-viewpoint structures.

2.1.6 Academic Applications of UAF

Recent academic research demonstrates expanding UAF application across defense and commercial domains. Eichmann et al. documented a UAF-based system-of-systems model development for an unmanned aircraft system [44]. Abhaya proposed a UAF-Based MBSE method for system-of-systems modeling [45]. Liu et al. presented top-down military system-of-systems design using MBSE based on UAF [46]. Torkjazi et al. addressed integrating autonomy into systems-of-systems using UAF [47].

These academic applications share a common characteristic: they address defense or aerospace systems rather than enterprise IT or Information Assurance. The UAF capabilities these researchers employ—multi-viewpoint modeling, requirements traceability, system-of-systems analysis—offer potential value for enterprise IT contexts. Yet the research community has not examined this application. The literature contains case studies, methodology proposals, and implementation guidance for physical systems. Enterprise IT and Information Assurance applications remain unexplored.

Yet despite this expanding academic utilization, enterprise IT and Information Assurance applications remain conspicuously absent from the research literature. The frameworks exist; the methodologies have matured; the tools have proliferated. But the research community has not applied these capabilities to the domains where visibility and documentation challenges persist most acutely.

2.2 Digital Engineering Foundational Literature

Digital Engineering has emerged as the preferred approach to complex system development across defense, aerospace, and related domains. This section examines the foundational guidance and strategic direction established by authoritative organizations including the Department of Defense, NASA, and INCOSE. Understanding this authoritative foundation establishes the conceptual framework within which Digital Engineering capabilities are defined and evaluated.

2.2.1 Department of Defense Digital Engineering Strategy

The Department of Defense Digital Engineering Strategy, published in June 2018, established the formal vision for transforming defense acquisition through Digital Engineering practices [27]. The strategy defines five strategic goals: formalize the development, integration, and use of models to inform enterprise and program decisions; provide an authoritative source of truth; incorporate technological innovation to improve engineering practice; establish a Digital Engineering ecosystem; and transform the culture and workforce to adopt Digital Engineering.

Each strategic goal warrants examination because together they define the full scope of Digital Engineering transformation. Goal 1 addresses model-based approaches, establishing that models should drive decision-making rather than merely documenting decisions already made. Goal 2 emphasizes authoritative sources of truth, recognizing that multiple disconnected documentation sources undermine confidence and accuracy. Goal 3 acknowledges that Digital Engineering must incorporate emerging technologies including artificial intelligence and advanced analytics. Goal 4 recognizes that Digital Engineering requires an ecosystem of tools, standards, and practices rather than isolated implementations. Goal 5 addresses the human dimension, acknowledging that technology adoption requires workforce transformation.

The authoritative source of truth concept deserves particular attention because it directly addresses the documentation-reality gap identified in Chapter 1. The DoD strategy defines the authoritative source of truth as “a single source of data and models” that provides “a definitive technical baseline” for programs [27]. This concept recognizes that multiple documentation sources inevitably diverge, creating the ambiguity and inconsistency that undermine both engineering decisions and compliance verification. Digital Engineering addresses this challenge by establishing single authoritative sources from which all views, reports, and analyses are generated.

DoD Instruction 5000.97, issued in December 2023, codifies Digital Engineering requirements for defense programs [48]. The instruction mandates that programs leverage digital artifacts as the authoritative source of system information, maintain digital thread capabilities throughout the acquisition lifecycle, and employ digital twins for system analysis and testing. This formal policy requirement demonstrates the maturation of Digital Engineering from strategic aspiration to mandated practice within defense acquisition.

The Systems Engineering Guidebook, published by the Office of the Under Secretary of Defense for Research and Engineering in February 2022, provides detailed implementation guidance for Digital Engineering practices within defense programs [17]. The guidebook addresses model-based systems engineering, digital thread implementation, digital twin employment, and the integration of these capabilities within program management and acquisition processes.

2.2.2 NASA Digital Engineering Implementation

NASA has implemented Digital Engineering across its mission portfolio through the Digital Engineering Acquisition Framework Handbook, NASA-HDBK-1004 [49]. The handbook provides guidance for incorporating Digital Engineering practices into NASA programs and acquisitions, addressing model-based approaches, digital thread requirements, and digital twin applications. NASA's experience demonstrates Digital Engineering value in civilian contexts requiring the same rigor and traceability as defense applications.

The NASA Model-Based Systems Engineering Vision and Strategy Bridge document establishes the agency's path toward pervasive MBSE adoption [28]. NASA's experience provides evidence of Digital Engineering value in complex mission-critical systems while documenting the organizational and technical challenges of enterprise adoption. The lessons NASA learned during MBSE adoption—cultural resistance, tool integration challenges, workforce development requirements—inform expectations for Digital Engineering adoption in other contexts.

NASA's independent development of Digital Engineering guidance parallel to DoD efforts validates the broad applicability of these methodologies. Both organizations confronted similar challenges: complex systems requiring thorough documentation, stringent compliance requirements demanding verifiable traceability, and mission-critical operations tolerating no ambiguity in system understanding. Both organizations converged upon Digital Engineering as the solution. This convergence suggests that Digital Engineering addresses core challenges of complex system management rather than domain-specific concerns unique to defense or space applications.

2.2.3 INCOSE Digital Engineering Vision

The International Council on Systems Engineering has positioned Digital Engineering as the future of the systems engineering discipline. The INCOSE Systems Engineering Vision 2035 document envisions model-based systems engineering becoming the dominant paradigm across all complex system development [50]. This vision extends beyond defense and aerospace to encompass all domains where systems engineering applies.

The INCOSE Systems Engineering Handbook, Fifth Edition, published in 2023, elaborates upon ISO/IEC/IEEE 15288:2023 life cycle processes with specific MBSE methodology guidance [51]. The handbook provides the authoritative reference for systems engineering practice, integrating Digital Engineering concepts throughout. The INCOSE Digital Engineering Information Exchange Working Group promotes collaboration and knowledge sharing among practitioners implementing Digital Engineering practices [16].

INCOSE's positioning of Digital Engineering as the future of systems engineering carries implications for fields beyond traditional systems engineering scope. As systems engineering expands to address enterprise systems, IT infrastructure, and organizational capabilities, Digital Engineering methodologies follow. The question becomes not whether Digital Engineering applies to enterprise IT and Information Assurance but when and how practitioners in these domains adopt methodologies that systems engineering has validated.

2.2.4 Systems Engineering Body of Knowledge

The Systems Engineering Body of Knowledge (SEBoK), jointly managed by INCOSE, IEEE Systems Council, and Stevens Institute's Systems Engineering Research Center (SERC), provides the globally recognized authoritative reference defining Digital Engineering's relationship to MBSE, digital threads, and authoritative source of truth within the ISO/IEC/IEEE 15288:2023 framework [52]. SEBoK establishes Digital Engineering concepts as core systems engineering knowledge, positioning them for broader adoption as systems engineering practices expand.

2.3 NIST and SERC Publications

The National Institute of Standards and Technology and the Systems Engineering Research Center have produced foundational publications supporting Digital Engineering and systems security engineering. This section examines key publications while noting the absence of guidance specifically addressing enterprise IT contexts.

2.3.1 NIST Framework for Cyber-Physical Systems

The NIST Framework for Cyber-Physical Systems, published as Special Publication 1500-201, provides relevant guidance for enterprise systems engineering [53]. The framework establishes a CPS analysis methodology based upon facets including conceptualization, realization, and assurance. Despite thorough treatment of cyber-physical considerations, the framework does not specifically address enterprise IT infrastructure or Information Assurance program management.

The cyber-physical systems focus reflects NIST's recognition that physical and digital systems increasingly converge. Industrial control systems, Internet of Things deployments, and operational technology environments blur boundaries between traditional IT and physical systems. The framework's analytical methodology offers potential application to enterprise IT contexts where similar convergence occurs. However, explicit guidance for such application does not exist in current NIST publications.

2.3.2 NIST Systems Security Engineering Publications

NIST's systems security engineering publications establish principles for engineering trustworthy secure systems. Special Publication 800-160 Volume 1 Revision 1 describes a basis for establishing principles, concepts, activities, and tasks for engineering systems that merit stakeholder trust [26]. Special Publication 800-160 Volume 2 Revision 1 complements Volume 1 by addressing cyber resiliency considerations [54].

These publications emphasize systems engineering approaches to security, recognizing that security outcomes depend upon how systems are designed and built rather than merely upon controls applied after deployment. This systems engineering perspective aligns with Digital Engineering's integrated approach. The publications reference model-based approaches and traceability requirements without providing specific implementation guidance for Digital Engineering in enterprise IT contexts.

The systems security engineering publications establish requirements that Digital Engineering could address. SP 800-160 requires traceability between security requirements, design decisions, and implementation artifacts. It requires documentation that maintains currency throughout system lifecycles. It requires visibility into system configurations and relationships. These requirements parallel Digital Engineering capabilities. Yet the publications do not explicitly connect these requirements to Digital Engineering solutions.

2.3.3 NIST Digital Twin Publications

NIST Internal Report 8356 addresses novel cybersecurity challenges and trust considerations for digital twin implementations [55]. NIST researchers have also contributed to ISO 23247 digital twin standards analysis [56]. These publications establish that NIST recognizes digital twin technology as relevant to cybersecurity while acknowledging the security challenges that digital twin implementations introduce.

The digital twin publications address security considerations for systems employing digital twins rather than digital twin applications to Information Assurance. The publications examine how to secure digital twin implementations rather than how digital twins might enhance security posture visibility or compliance verification. This distinction reflects the current state of research: digital twins are examined as systems to be secured rather than as tools for improving security operations.

2.3.4 Systems Engineering Research Center Technical Reports

The Digital Engineering Competency Framework, documented in technical report SERC-2021-TR-005, defines 962 Knowledge, Skills, Abilities, and Behaviors organized by proficiency levels [20]. The Digital Engineering Metrics technical report, SERC-2020-TR-002, develops frameworks for measuring Digital Engineering benefits and adoption [19]. Additional SERC technical reports address enterprise system-of-systems modeling and systems engineering modernization [57], [58].

The SERC technical reports provide the academic foundation for Digital Engineering practice. The competency framework informs workforce development. The metrics framework enables organizations to measure adoption progress and benefits realization. These frameworks support Digital Engineering implementation in any domain, including enterprise IT and Information Assurance, though specific application guidance for these domains does not exist in current SERC publications.

2.4 Model-Based Systems Engineering Research

Model-Based Systems Engineering represents a paradigm shift from document-centric to model-centric systems engineering practices. This section examines the evidence base for MBSE value, adoption challenges, and the absence of research addressing enterprise IT applications.

2.4.1 Systematic Reviews of MBSE Evidence

The most comprehensive assessment of MBSE evidence comes from Wooley and Womack, whose 2025 systematic literature review analyzed adoption, benefits, and challenges across the MBSE research corpus [59]. The review explicitly notes the absence of research addressing enterprise IT infrastructure or Information Assurance applications. This finding validates that the research gap identified in this dissertation reflects the actual state of academic literature rather than incomplete literature search.

The systematic review identified consistent themes across MBSE research: improved requirements traceability, enhanced communication among stakeholders, better design validation, and more effective change management. These benefits address challenges documented in enterprise IT and Information Assurance contexts. Yet researchers have not examined whether benefits demonstrated in aerospace and defense contexts transfer to enterprise IT applications.

Earlier systematic reviews by Henderson and Salado examined MBSE value and maturity across industrial contexts [60]. Wolny et al. reviewed empirical evidence for model-based methods [61]. Chami and Bruel surveyed MBSE tools and applications [62]. These reviews collectively establish that MBSE has demonstrated value across multiple domains while documenting the absence of enterprise IT applications.

2.4.2 Empirical Studies of MBSE Implementation

Research by Gregory et al. examined model-based engineering practices within defense programs, documenting improved requirements traceability and more effective design reviews but also identifying organizational and technical barriers to adoption [63]. The empirical evidence indicates that MBSE provides value in traditional systems engineering domains. However, the transferability of these benefits to enterprise IT and Information Assurance domains remains unexamined.

The adoption barriers identified in MBSE research warrant attention because similar barriers likely impede adoption in enterprise IT contexts. Cultural resistance to new methodologies, tool learning curves, initial productivity decreases during transition, and integration challenges with existing processes all affected MBSE adoption in aerospace and defense. Organizations considering MBSE for enterprise IT applications should anticipate similar challenges.

2.4.3 SysML and Modeling Language Research

The Systems Modeling Language (SysML) provides the predominant modeling language for MBSE implementations. Research by Friedenthal et al. establishes SysML as the practical standard for systems engineering modeling [64]. SysML extends the Unified Modeling Language (UML) with constructs for requirements, parametrics, and system structure that UML lacks. This extension makes SysML suitable for systems engineering applications where UML's software focus proves insufficient.

The evolution from SysML 1.x to SysML v2 addresses limitations that impeded broader adoption. SysML v2 improves precision, expressiveness, and usability through a redesigned language architecture. The new version provides better support for tool interoperability through standardized APIs and textual notation. These improvements may reduce barriers to MBSE adoption in domains beyond traditional systems engineering.

2.4.4 The Absence of MBSE for Enterprise IT

The literature review reveals a striking gap: no peer-reviewed research addresses MBSE application to enterprise IT infrastructure or Information Assurance program management. With the sole exception of the reference model by Bonar and Hastings, the academic literature contains no studies examining whether MBSE approaches could improve IT service management, enhance security control implementation, or support compliance verification in enterprise contexts [29].

This absence is particularly notable given the explicit requirements within compliance frameworks for architectural documentation, requirements traceability, and configuration management that MBSE provides. NIST publications require enterprise architecture capabilities. ITIL frameworks assume configuration management accuracy. Yet researchers have not examined whether MBSE could address these requirements more effectively than traditional approaches.

2.5 Digital Twin Technology

Digital twin technology has emerged as a transformative capability across multiple domains. This section examines digital twin foundations, standards development, and security applications.

2.5.1 Digital Twin Foundations

Grieves traces the evolution of digital twin concepts from Product Lifecycle Management origins through contemporary applications [65]. Grieves, who originated the digital twin concept, positions it as the integration of physical and virtual systems that enables analysis, optimization, and prediction. Research by Madni and Sievers provides a framework for leveraging digital twins in systems engineering contexts [24]. Khan et al. examine digital twin applications in emerging technology contexts [25].

The foundational research establishes digital twins as more than simulation or modeling. Digital twins maintain synchronization with physical counterparts through continuous data exchange. This synchronization distinguishes digital twins from static models and enables the real-time analysis and prediction that static approaches cannot provide.

2.5.2 Digital Twin Standards Development

Shao examines ISO 23247 and IEC 62832 standards for digital twin frameworks [23]. Shao et al. provides additional analysis of ISO 23247's four-part structure [56]. These standards establish interoperability requirements for digital twin implementations, addressing data exchange, interface specifications, and functional requirements.

The standards development activity indicates maturing technology readiness for enterprise adoption. Standardized interfaces reduce vendor lock-in concerns. Common data models enable integration across digital twin implementations. These standards provide foundation for digital twin adoption beyond the aerospace and manufacturing contexts where the technology originated.

2.5.3 Digital Twin Security Applications

Eckhart and Ekelhart review digital twins for cyber-physical systems security [66]. Karaarslan and Babiker examine digital twin security threats and countermeasures [67]. Vielberth et al. propose a digital twin-based cyber range for SOC analyst training [68]. Dietz and Pernul examine digital twins for enterprise security [69].

This emerging research addresses digital twins as security tools rather than merely systems requiring security. The cyber range application demonstrates digital twin value for security operations training. The enterprise security examination begins exploring digital twin application to organizational security postures. These preliminary investigations suggest research interest in digital twins for Information Assurance applications, though comprehensive studies remain absent.

2.6 Barriers to Digital Engineering Adoption Beyond Defense and Aerospace

Despite demonstrated value in defense and aerospace contexts, Digital Engineering has not achieved widespread adoption in enterprise IT, commercial organizations, or Information Assurance programs. Understanding the barriers to broader adoption illuminates why the research gap documented in this literature review persists.

2.6.1 Platform-Centric versus Enterprise Adoption Patterns

Digital Engineering adoption in defense and aerospace has concentrated upon platform and mission-specific applications. Aircraft programs, spacecraft missions, and weapons systems have implemented Digital Engineering practices. Enterprise IT functions within these same organizations have not. This pattern suggests that Digital Engineering adoption occurs where systems engineering disciplines are established rather than extending to IT domains that historically operated independently.

The platform-centric adoption pattern reflects how Digital Engineering initiatives originate. Program managers facing acquisition challenges adopt Digital Engineering to improve program outcomes. Systems engineers seeking better requirements traceability implement MBSE. These adoption decisions occur at program level rather than enterprise level. Enterprise IT organizations, operating separately from program organizations, do not participate in these adoption decisions and do not benefit from resulting capabilities.

Research by Campagna et al. examined strategic adoption of digital innovations, finding that digital transformation requires coordinated enterprise-level application rather than bottom-up adoption of individual technologies [70]. The research identifies twelve strategic adoption influencers and notes that adoption research focuses upon individual technologies rather than integrated digital transformation. This finding explains why platform-level Digital Engineering adoption has not expanded to enterprise IT: the enterprise coordination required for such expansion does not occur.

2.6.2 Organizational Barriers to Adoption

Multiple organizational factors impede Digital Engineering adoption in enterprise IT contexts. First, enterprise IT organizations typically lack systems engineering heritage. Systems engineering practices including MBSE developed within engineering organizations addressing physical systems. IT organizations evolved from data processing and network management traditions with different practices, tools, and professional identities. Adopting Digital Engineering requires IT professionals to adopt practices from an unfamiliar discipline.

Second, organizational structures separate IT from engineering functions. Defense organizations employ systems engineers in program offices and IT professionals in separate enterprise IT organizations. These organizational units report through different chains, operate under different governance, and possess different cultures. Digital Engineering capabilities developed by engineering organizations do not automatically transfer to IT organizations operating independently.

Third, IT governance frameworks do not incorporate Digital Engineering concepts. ITIL, COBIT, and other IT management frameworks do not reference MBSE, digital threads, or model-based documentation. IT professionals seeking guidance from established frameworks find no direction toward Digital Engineering adoption. This framework gap perpetuates traditional approaches even when Digital Engineering might address documented challenges more effectively.

2.6.3 Technical Barriers to Adoption

Technical factors also impede adoption. Digital Engineering tools developed for aerospace and defense applications do not integrate readily with enterprise IT management tools. MBSE platforms like Cameo and Rhapsody do not interface with IT service management platforms like ServiceNow or BMC. This tool gap requires custom integration efforts that increase adoption costs and complexity.

Additionally, modeling languages developed for systems engineering do not directly accommodate enterprise IT constructs. SysML provides excellent support for modeling physical systems with requirements, behaviors, and structures. Modeling IT services, network configurations, and security controls requires adaptation or extension that practitioners must develop themselves. The absence of standardized approaches for modeling enterprise IT in SysML increases adoption barriers.

2.6.4 Economic Barriers to Adoption

Economic factors further impede adoption. Digital Engineering implementations require considerable investment in tools, training, and organizational transformation. Organizations must justify these investments against competing priorities. For aerospace programs with multi-billion-dollar budgets and decade-long timelines, Digital Engineering investments represent small fractions of program costs with measurable potential returns. For enterprise IT organizations operating on annual budgets with continuous delivery expectations, similar investments represent larger relative commitments with less certain returns.

The return on investment for Digital Engineering in enterprise IT contexts remains undemonstrated. Aerospace and defense organizations can cite program outcomes—reduced rework, improved first-pass quality, faster development cycles—to justify continued investment. Enterprise IT organizations have no comparable evidence because no research examines Digital Engineering benefits in these contexts. Without evidence, investment decisions favor proven approaches over experimental adoptions.

2.7 Open Source Standards and Tools for Digital Engineering

The availability of open source standards and tools influences adoption decisions by reducing costs, avoiding vendor lock-in, and enabling community-driven development. This section examines open source options for MBSE, digital threads, digital twins, and Product Lifecycle Management while assessing the research evidence supporting their adoption.

2.7.1 Open Source MBSE Tools

Several open source MBSE tools have emerged, primarily through the Eclipse Foundation's modeling ecosystem. Eclipse Papyrus provides an open source UML and SysML modeling environment based upon the Eclipse platform [71]. Capella, developed by Thales and contributed to Eclipse, provides a comprehensive MBSE tool based upon the Arcadia methodology [72]. SysON, currently under development, implements OMG's SysML v2 specification with modern web-based architecture [73].

These open source tools provide alternatives to commercial MBSE platforms like Cameo and Rhapsody. Capella has achieved significant industrial adoption, with deployments across aerospace, energy, transportation, and other sectors. The Eclipse Foundation's support provides organizational stability and community governance that individual open source projects may lack.

However, open source MBSE tools address traditional systems engineering applications. Documentation, examples, and community support focus upon aerospace, defense, and manufacturing applications. Organizations seeking to apply these tools for enterprise IT or Information Assurance must adapt without domain-specific guidance. The tools are capable; the application knowledge for enterprise IT contexts does not exist.

2.7.2 Open Source Digital Twin Frameworks

The Digital Twin Consortium has established an open source collaboration initiative providing frameworks and examples for digital twin development [74]. Eclipse Ditto provides an open source framework for creating and managing digital twins for IoT applications [75]. Eclipse BaSyx implements the Asset Administration Shell standard for industrial digital twins [76].

Academic research has examined open source digital twin frameworks. Gil et al. conducted a systematic survey of open source digital twin frameworks, analyzing fourteen frameworks against criteria derived from ISO 23247 standards [77]. The research found that open source options exist but vary significantly in maturity, documentation quality, and community support. The survey provides guidance for organizations evaluating open source digital twin options.

Research by Autiosalo et al. introduced Twinbase, an open source server for the Digital Twin Web concept [78]. This academic research demonstrates that open source digital twin development attracts scholarly attention, though applications focus upon manufacturing and IoT rather than enterprise IT.

2.7.3 Open Source PLM Options

Product Lifecycle Management has historically been dominated by proprietary vendors including Siemens, Dassault Systmes, and PTC. Open source alternatives have emerged but have not achieved comparable adoption. Aras Innovator pioneered enterprise open source PLM, offering its platform through subscription models with open access to source code [79]. OpenPLM and DocDokuPLM provide fully open source alternatives with more limited functionality and adoption.

Academic research on open source PLM remains limited. Laili et al. examined industrial open source solutions for product lifecycle management, identifying standardization challenges and integration requirements [80]. The research notes that PLM open source adoption faces barriers including integration complexity, limited community support compared to commercial options, and enterprise requirements that open source solutions may not fully address.

For enterprise IT applications, PLM concepts face the same applicability challenges as MBSE. PLM tools and practices developed for physical product management do not directly accommodate information system lifecycle management. Open source availability does not resolve this structural scope limitation.

2.7.4 Research Evidence for Open Source Digital Engineering Adoption

The research evidence supporting open source Digital Engineering adoption consists primarily of gray literature—vendor documentation, consortium publications, and practitioner reports—rather than peer-reviewed academic research. Academic studies examining open source MBSE tools exist but focus upon aerospace and defense applications. Academic studies of open source digital twin frameworks exist but address manufacturing and IoT rather than enterprise IT.

No peer-reviewed academic research examines open source Digital Engineering adoption for enterprise IT or Information Assurance applications. The research gap identified throughout this literature review extends to open source contexts. Whether open source tools could enable Digital Engineering adoption in resource-constrained organizations remains an open question without empirical investigation.

This absence of academic research creates uncertainty for organizations considering adoption. Commercial vendor claims of Digital Engineering benefits may reflect marketing rather than validated outcomes. Gray literature from industry and working groups may reflect advocacy rather than objective assessment. Without academic research, organizations cannot rely upon peer-reviewed evidence to inform adoption decisions for enterprise IT applications.

2.8 Information Assurance and Compliance Frameworks

Information Assurance frameworks establish requirements for protecting information systems and demonstrating compliance. This section examines the NIST Risk Management Framework and related compliance mechanisms.

2.8.1 NIST Risk Management Framework

The NIST Risk Management Framework, documented in Special Publication 800-37 Revision 2, provides the authoritative approach to managing security and privacy risk for federal information systems [81]. The RMF establishes seven iterative steps: prepare, categorize, select, implement, assess, authorize, and monitor.

The RMF explicitly requires enterprise architecture integration. Organizations must determine system placement within enterprise architecture during the prepare step. Yet compliance with this requirement assumes capabilities that organizations demonstrably lack: the ability to maintain accurate, current documentation of enterprise architecture that reflects operational reality. Digital Engineering could address this requirement through model-based documentation that maintains currency automatically. However, no guidance exists for applying Digital Engineering to RMF compliance.

2.8.2 NIST SP 800-53 Security Controls

NIST Special Publication 800-53 Revision 5 provides the security control catalog for federal information systems [3]. Multiple controls explicitly require enterprise architecture capabilities: PL-2 requires security plans consistent with enterprise architecture; PL-8 requires security architecture development; PM-7 establishes enterprise architecture requirements; CM-2 requires documented baselines; CM-8 requires accurate system component inventory; SA-17 requires design specifications consistent with enterprise architecture.

These control requirements establish compliance obligations that Digital Engineering could address. Security plans maintained within MBSE models could ensure consistency with enterprise architecture. Security architectures developed using UAF could satisfy PL-8 requirements. Configuration baselines managed through PLM approaches could address CM-2 and CM-8 requirements. Yet no research examines Digital Engineering approaches to satisfying these specific controls.

2.8.3 CNSSI 1253 for National Security Systems

The Committee on National Security Systems Instruction 1253 provides security categorization and control selection guidance for national security systems [82]. National security systems face the same documentation and visibility challenges as other information systems while operating under additional constraints that complicate compliance. Digital Engineering approaches that enhance compliance verification could provide particular value for national security system operators who must demonstrate compliance to multiple oversight bodies.

2.8.4 ISO 27001 and Alternative Frameworks

Organizations outside federal requirements may employ alternative security control frameworks. ISO/IEC 27001:2022 provides an international standard for information security management systems [11]. These alternative frameworks share common characteristics with NIST guidance: they assume documentation accuracy and visibility capabilities that organizations struggle to maintain. Digital Engineering could address documentation requirements across frameworks regardless of which specific framework organizations employ.

2.8.5 OSCAL and Automation Initiatives

The NIST Open Security Controls Assessment Language (OSCAL) represents an initiative to enable automated compliance verification through machine-readable security documentation [83]. OSCAL provides standardized formats for expressing security control catalogs, baselines, profiles, and assessment results. This automation initiative aligns with Digital Engineering's emphasis upon machine-readable documentation that enables automated processing.

OSCAL demonstrates recognition within the compliance community that manual documentation approaches cannot sustain accuracy and currency requirements. The initiative provides foundation for automated compliance verification that Digital Engineering could extend. Digital thread traceability could connect OSCAL compliance documentation to underlying system configurations, enabling automated verification that documented controls exist as implemented.

2.9 IT Service Management Literature

IT Service Management frameworks establish practices for delivering IT services effectively across the enterprise. This section examines ITIL requirements, configuration management challenges, and persistent failures that undermine IT service delivery.

2.9.1 ITIL Framework Requirements

The Information Technology Infrastructure Library provides guidance for IT service management [4]. ITIL 4 reorganized service management practices and introduced the Service Value System concept [84]. Despite recognizing that tracking configurations across virtual systems, cloud computing, and cybersecurity domains presents challenges, ITIL provides limited guidance on addressing documentation accuracy challenges.

ITIL assumes that organizations can maintain accurate configuration information, implement effective change management, and coordinate service delivery across complex environments. These assumptions underlie ITIL practices for incident management, problem management, and service continuity. When assumptions fail—when configuration information is inaccurate, when change impacts are miscalculated, when service dependencies are undocumented—ITIL practices cannot deliver intended value.

2.9.2 Configuration Management Database Challenges

Configuration Management Database implementation failures stand extensively documented in industry research. Gartner reports an eighty percent failure rate for CMDB implementations [12]. Additional research indicates that ninety-nine percent of organizations using CMDB tooling without addressing data quality gaps will experience visible business disruption [85]. Forrester research finds that less than half of organizations trust the data in their CMDB [86].

Data quality statistics reveal the core challenge: sixty percent of data manually input by employees proves inaccurate [87]. Five problem areas persist: missing assets, duplicate assets, incomplete configuration item records, missing relationships, and stale data. These data quality problems reflect inherent limitations of manual documentation approaches rather than implementation failures that improved processes could address.

Recent analysis concludes that the CMDB approach itself has failed [88]. After decades of implementation attempts across organizations, CMDBs consistently fail to deliver intended value. The analysis attributes failures to structural issues: involving process experts rather than data management professionals, manual data entry that cannot maintain accuracy, and scope creep that renders CMDBs unmanageable. This assessment suggests that incremental CMDB improvements cannot resolve inherent approach limitations.

2.9.3 Academic Research on ITIL Implementation

Cook et al. found resistance to change at twenty-seven percent as the top ITIL implementation challenge [89]. Marrone and Kolbe surveyed 491 firms finding that while over ninety percent use ITSM frameworks, little research examines actual benefits realized [90]. Research by Benbya et al. demonstrates that enterprise information systems have reached complexity levels exceeding prior technological generations [6].

These academic studies document ITIL adoption and implementation challenges without examining Digital Engineering as a potential solution. The research establishes that ITIL implementations face challenges and that benefits remain uncertain. However, researchers have not investigated whether model-based approaches, digital threads, or other Digital Engineering capabilities could improve ITIL implementation outcomes.

2.9.4 Shadow IT and Documentation Accuracy

Gartner research indicates forty-one percent of employees used shadow IT in 2022, expected to climb to seventy-five percent by 2027 [14]. Thirty to forty percent of large companies' IT expenditure represents shadow IT. Shadow IT undermines configuration management because systems deployed without IT oversight cannot be documented. No manual process can maintain awareness of systems that bypass official acquisition and deployment channels.

The shadow IT phenomenon reflects a structural mismatch between IT governance and organizational needs. When official IT processes cannot meet user requirements quickly enough, users acquire solutions independently. These solutions become operational dependencies that official documentation does not capture. The documentation-reality gap widens automatically as shadow IT proliferates.

2.9.5 Change Management and Impact Assessment

Industry analysis confirms that reliance upon outdated documentation leads to inaccurate impact assessments [91]. Research by Bokan and Santos highlights difficulties organizations encounter in maintaining comprehensive security oversight [7]. Change management depends upon accurate understanding of system relationships [92] that current documentation approaches cannot maintain.

The relationship between documentation accuracy and change management effectiveness deserves emphasis. Every change approved based upon inaccurate documentation represents a potential incident. When impact assessments miss dependencies that exist in operational systems, changes cause unintended effects. The resulting incidents consume resources, damage trust in change processes, and create pressure for emergency changes that further degrade documentation accuracy.

2.9.6 Integration with Information Assurance

Thompson et al. examined integrating MBSE with IT Service Management [93]. Previous research by Bonar and Hastings demonstrated that compliance verification is enhanced by Digital Engineering practices [29]. These preliminary investigations suggest that integration between Digital Engineering and IT Service Management offers value, though comprehensive research remains absent.

2.10 Enterprise Visibility and Dependency Documentation Failures

The challenges documented in preceding sections share common roots in the inability of organizations to maintain accurate, current documentation of their enterprise information systems. This section synthesizes peer-reviewed research and industry analysis to establish why traditional practices fail to trace, model, and document service dependencies across enterprise environments. Understanding these root causes provides the foundation for evaluating Digital Engineering as a potential solution.

2.10.1 Documented Scope of Visibility Failures

Research consistently documents that organizations lack visibility into large portions of their IT environments. IDC and Exabeam found that organizations globally can monitor only sixty-six percent of their IT environments, leaving blind spots particularly in cloud deployments [13]. The Ponemon Institute's 2023 Global Study on Closing the IT Security Gap found that sixty-three percent of security teams lack visibility and control into all user device activity connected to their infrastructure [94]. The SANS Institute SOC Survey found that only fifteen percent of respondents expressed very high confidence that all devices on their network are discoverable [95].

These visibility gaps compound across organizational boundaries. Ivanti's 2025 State of Cybersecurity Trends Report found that fifty-five percent of organizations maintain security and IT data silos, with sixty-two percent reporting that silos slow security response times [96]. The Cloud Security Alliance's 2024 study revealed that ninety-five percent of organizations suffered cloud-related breaches in the preceding eighteen months [97]. Check Point's 2024 Cloud Security Report found that eighty-two percent of enterprises experienced security incidents due to cloud misconfigurations, while sixty-seven percent struggle with limited visibility into cloud infrastructure [98].

A notable discrepancy exists between peer-reviewed and industry research regarding the sources of these visibility failures. Peer-reviewed research by Hauder et al. attributes documentation challenges primarily to manual processes and data quality issues, while industry reports often emphasize tool limitations [99]. This discrepancy may reflect different analytical perspectives: academic research examines root causes while industry research often focuses upon symptoms addressable through commercial solutions. The evidence consistently supports that both manual process limitations and tool inadequacies contribute to visibility failures.

2.10.2 Configuration Drift and Baseline Divergence

Peer-reviewed research provides empirical evidence for configuration-related failures. Yin et al. conducted an empirical study published in ACM's Symposium on Operating Systems Principles examining configuration errors in commercial and open source systems [100]. Their analysis found that seventy to eighty-five percent of misconfigurations result from mistakes in setting configuration parameters. Their research revealed that twenty-two to fifty-seven percent of misconfigurations involve configurations external to the examined system, some on entirely different hosts—demonstrating the dependency documentation challenge that extends beyond individual system boundaries.

NIST Special Publication 800-128, Guide for Security-Focused Configuration Management, defines configuration drift as systems deviating from baseline configurations over time through manual interventions, software updates, and environmental factors [101]. The publication establishes that effective security configuration management requires continuous monitoring—a capability most organizations lack.

The Uptime Institute's Annual Outage Analysis provides validation of these failures: sixty-four percent of IT system and software-related outages detected worldwide occurred because of configuration or change management issues [102]. The IT Process Institute's Visible Ops Handbook established that eighty percent of unplanned outages result from ill-planned changes made by administrators or developers [103]—changes that proper dependency documentation would have flagged.

2.10.3 Detection Time as Visibility Indicator

Breach detection times serve as proxy measures for organizational visibility into their information systems. IBM Security and Ponemon Institute report that the mean time to identify breaches reached two hundred four days, with breaches involving lifecycles exceeding two hundred days costing an average of 5.46 million dollars [15]. The 2024 report found that only forty-two percent of breaches were detected internally. Stolen credential breaches—reflecting authentication and identity management documentation failures—required two hundred ninety-two days to identify and contain, the longest of any attack vector.

The 2025 report identified that thirty-five percent of breaches involved shadow data—information stored in unmanaged locations—and forty percent of breaches involved data stored across multiple environments that organizations struggle to inventory comprehensively [104]. These findings demonstrate that visibility failures directly impact security outcomes. Organizations that cannot see their systems cannot protect them effectively.

2.10.4 Organizational Silos and Fragmented Visibility

Peer-reviewed research provides theoretical frameworks for understanding why visibility gaps persist. Bento et al. conducted a scoping review of forty studies on organizational silos, identifying five conceptualizations: formal units, functions, knowledge areas, technologies, and broad definitions [105]. The authors characterize silo mentality as an absence of systems thinking and organizational vision, identifying silos as barriers to achieving organizational goals. Their review applies complexity theory, social network analysis, and Bandura's reciprocal determinism model to demonstrate that structure, process, and function factors all contribute to silo persistence.

Hauder et al. conducted peer-reviewed research on enterprise architecture documentation challenges, finding that EA documentation is performed manually to a large extent, making the process time-consuming, error-prone, and requiring collection of quality data [99]. Their study identified four categories of challenges based on industry examples, literature review, and a survey of 123 EA practitioners.

Brée and Karger conducted a systematic literature review examining enterprise architecture management challenges [106]. Their review organized EAM tasks into six dimensions: EA documentation, EA planning, EA communication/support, EA programming, EA implementation, and EA governance. Documentation challenges identified include dearth of automated tools, immature documentation models, and insufficient emphasis on forward-looking documentation.

2.10.5 Complexity Theory Perspective

Complexity theory provides a framework for understanding why traditional documentation approaches fail in modern enterprise environments. Benbya and McKelvey applied Complex Adaptive Systems theory to information systems development, arguing that ISD complexity is magnified by continuous changes in user requirements [107]. Their framework proposes seven first principles of adaptive success: adaptive tension, requisite complexity, change rate, modular design, positive feedback, causal intricacy, and coordination rhythm. The authors argue that if complexity is not managed appropriately, information systems fail.

Enterprise IT environments exhibit characteristics of complex adaptive systems: numerous interconnected components, emergent behaviors arising from component interactions, continuous change, and unpredictable responses to interventions. Static documentation approaches assume systems remain stable between documentation updates—an assumption that fails in environments exhibiting complex adaptive system characteristics.

2.10.6 Technical Debt in Documentation Domains

Peer-reviewed research on technical debt provides additional perspective on documentation failures. Santos et al. specifically addressed documentation technical debt—problems concerning non-existent, inadequate, or incomplete software project documentation [108]. Their qualitative study identified causes, consequences, and best practices to avoid documentation problems.

Li et al. conducted a systematic mapping study covering ninety-four studies that established technical debt taxonomy and management frameworks [109]. Their taxonomy includes architecture, design, code, test, and documentation debt as distinct categories. Junior and Travassos consolidated perspectives on technical debt across nineteen secondary studies [110]. Kleinwaks extended TD concepts to systems engineering contexts [111].

Documentation technical debt accumulates when organizations defer documentation updates to prioritize operational activities. Unlike code technical debt, documentation debt remains invisible until documentation is needed for change impact assessment, incident response, or compliance verification. The accumulated debt then imposes costs far exceeding the original deferral savings.

2.10.7 CMDB Failure Analysis

The widely-cited eighty percent CMDB failure rate from Gartner research warrants examination against peer-reviewed evidence. Betz analyzed CMDB failures, concluding that the CMDB approach has failed after multiple implementation attempts across organizations [88]. The analysis attributes failures to involving process experts rather than data management professionals. Forrester's research on Application and Infrastructure Dependency Mapping found that fifty-six percent of enterprises report incomplete views of dependencies between applications and underlying infrastructure [112].

Peer-reviewed research by Hauder et al. provides corroborating evidence from academic study of 123 practitioners, finding that manual documentation processes cannot maintain accuracy in dynamic environments [99]. The convergence of industry and academic findings supports the conclusion that CMDB approaches face structural limitations rather than merely implementation challenges.

2.10.8 Summary of Enterprise Visibility Evidence

Table 2.1 summarizes the evidence documenting enterprise visibility and documentation failures across peer-reviewed and industry research sources. The statistics demonstrate consistent patterns: organizations lack comprehensive visibility into their IT environments, documentation accuracy remains poor despite investment, and the resulting gaps create measurable impacts on security outcomes and operational effectiveness.

Table 2.1: Enterprise Visibility and Documentation Failure Evidence

Finding	**Statistic**	**Source**
	Visibility Gap Metrics	
IT environment monitorable	66%	IDC/Exabeam 2023[13]
Security teams lacking device visibility	63%	Ponemon Institute 2023[94]
High confidence in device discovery	15%	SANS Institute 2023[95]
Organizations with security/IT silos	55%	Ivanti 2025[96]
	Configuration Management Failures	
CMDB implementation failure rate	80%	Gartner Research[12], [85]
Outages from configuration issues	64%	Uptime Institute 2023[102]
Misconfigurations from parameter errors	70-85%	Yin et al. 2011[100]
Unplanned outages from ill-planned changes	80%	IT Process Institute[103]
	Shadow IT and Undocumented Assets	
Shadow IT as percentage of IT spend	30-40%	Gartner Research[14]
Cloud services vs. IT estimates	15-22x higher	Cisco 2016[113]
Employees using shadow IT (2022)	41%	Gartner Research[14]
Projected shadow IT usage (2027)	75%	Gartner Research[14]
	Security Impact Metrics	
Mean time to identify breach	204 days	IBM/Ponemon 2024[15]
Cloud breaches from misconfigurations	82%	Check Point 2024[98]
Organizations with cloud breaches (18 mo)	95%	CSA 2024[97]
Projected preventable cloud breaches (2027)	99%	Gartner Research[114]

The convergence of peer-reviewed empirical research and industry analysis establishes that enterprise visibility and documentation failures represent a systemic challenge rather than isolated organizational deficiencies. Traditional documentation approaches—manual configuration tracking, periodic documentation updates, static architecture diagrams—cannot maintain accuracy in environments characterized by continuous change, complex dependencies, and organizational silos. This evidence base establishes the problem space that Digital Engineering may address.

2.11 Security Architecture and Threat Modeling

Security architecture documentation and threat modeling practices determine how organizations understand their defensive postures and identify vulnerabilities. This section examines current approaches and the emerging application of MBSE to security domains.

2.11.1 Security Architecture Documentation Practices

Security architecture documentation traditionally relies upon static artifacts including network diagrams, data flow diagrams, and textual descriptions. Research by Hassan and Bahgat examined frameworks for translating high-level security policy into low-level security mechanisms [115]. The gap between security architecture documentation and operational configuration represents a persistent challenge that current practices do not adequately address.

Security architectures document intended defensive postures. Operational configurations implement actual defensive postures. When these diverge—when documentation describes controls that are not implemented, or when implementations differ from documented specifications—security assurance degrades. Organizations cannot verify security postures by examining documentation when documentation does not reflect reality.

2.11.2 Threat Modeling with MBSE

Apvrille and Roudier proposed SysML-SecA, a methodology combining SysML with security analysis techniques [116]. This approach enables threat modeling integrated with system architecture models. The integration ensures that threat models remain connected to architecture models, updating as architectures evolve rather than diverging as static threat models do.

This research represents preliminary investigation of MBSE for security applications. The methodology addresses threat modeling for systems under development rather than enterprise IT environments already in operation. Adaptation for enterprise IT contexts would require extensions that current research has not examined.

2.11.3 Security Control Traceability

The ability to trace security requirements through control implementation to compliance evidence represents a persistent challenge. Digital threads could address this traceability challenge by maintaining verified connections between security requirements, control implementations, and compliance artifacts. However, research has not examined practical implementation of digital thread capabilities in Information Assurance contexts.

The traceability challenge manifests throughout the RMF lifecycle. During control selection, organizations must trace categorization decisions to appropriate control baselines. During implementation, organizations must trace selected controls to technical configurations. During assessment, organizations must trace configurations to evidence demonstrating effectiveness. During continuous monitoring, organizations must maintain these traces as systems evolve. Current practices provide no automated support for maintaining this traceability chain.

2.12 Research Gaps and Theoretical Framework

The systematic literature review reveals a pattern: frameworks and compliance requirements assume documentation and visibility capabilities that organizations demonstrably lack. This section synthesizes findings into a theoretical framework while documenting research gaps that this investigation begins to address.

2.12.1 Absence of Digital Engineering for Enterprise IT

The academic research gap is pronounced. Systematic literature reviews examining MBSE consistently find no research addressing enterprise IT infrastructure or Information Assurance applications. The sole exception is the reference model by Bonar and Hastings [29]. This gap persists despite explicit requirements in compliance frameworks for capabilities that Digital Engineering provides.

The gap cannot be attributed to Digital Engineering immaturity. Defense and aerospace have employed Digital Engineering successfully for years. The gap cannot be attributed to tool unavailability. MBSE tools, digital twin platforms, and PLM systems have existed for decades. The gap reflects a disciplinary boundary: systems engineering and IT have evolved as separate disciplines with limited cross-pollination.

2.12.2 Standards-Research Disconnect

Standards bodies have recognized enterprise applicability of systems engineering approaches. UAF provides viewpoints applicable to enterprise IT. NIST publications require enterprise architecture capabilities for compliance. ITIL requires visibility and documentation that model-based approaches could provide. Yet academic research has not examined practical application. This disconnect leaves practitioners without empirical guidance for applying available standards to enterprise IT challenges.

2.12.3 Summary of Research Gaps

Table 2.2 summarizes the research gaps identified across the literature domains examined in this review.

Table 2.2: Research Gaps Within Corpus of Knowledge

Domain	**Gap Description**	**Research Implication**
MBSE	One study applying MBSE to enterprise IT, none for IA	Foundation research required
Digital Threads	No research on traceability for IT/IA contexts	Conceptual validation needed
Digital Twin	Limited enterprise IT application research	Application studies needed
ITSM Integration	No frameworks integrating DE with ITIL	Integration research required
Compliance	No DE approaches for RMF compliance	Practical implementation studies
Open Source	No academic validation for enterprise IT	Evaluation research needed
Professional Perceptions	Unknown awareness and perceived value	This research addresses

2.13 Theoretical Framework

Based upon the systematic literature review, this research adopts a theoretical framework integrating Digital Engineering principles with established Information Assurance and IT Service Management practices. This framework posits that Digital Engineering represents a disciplinary approach capable of addressing gaps that have persisted despite decades of framework development and organizational investment.

2.13.1 Digital Engineering as Disciplinary Solution

The persistent failures documented in IT Service Management and Information Assurance practices share common root causes that Digital Engineering practices directly address. Organizations struggle with documentation accuracy because traditional approaches rely upon manual processes disconnected from operational systems. Organizations fail to maintain traceability because document-centric methods cannot sustain verified connections as systems evolve. Organizations lack visibility because static artifacts cannot represent dynamic system states.

2.13.1.1 Addressing the Authoritative Source of Truth Gap

The DoD Digital Engineering Strategy defines the authoritative source of truth as a single source of data and models providing a definitive technical baseline [27]. Current IT and Information Assurance practices lack authoritative sources of truth, instead maintaining multiple disconnected documentation artifacts that diverge over time. Digital Engineering's emphasis upon authoritative sources addresses this gap by establishing single, model-based repositories from which all views and reports are generated.

2.13.1.2 Addressing the Traceability Gap

Digital threads establish and maintain authoritative traceability throughout system lifecycles. Current Information Assurance practices struggle to maintain traceability between security requirements, security controls, technical configurations, and evidence demonstrating effectiveness. Digital thread capabilities address this gap by maintaining verified, bidirectional connections that update as systems evolve rather than requiring manual maintenance.

2.13.1.3 Addressing the Visibility Gap

Visibility into system configurations, dependencies, and states represents a core requirement for both IT Service Management and Information Assurance. Current practices fail to provide this visibility, with research documenting eighty percent CMDB failure rates and pervasive shadow IT [12], [14]. Model-based approaches that maintain synchronization with operational systems address this gap by providing visibility that manual documentation cannot sustain.

2.13.1.4 Addressing the Simulation and Testing Gap

Digital twin capabilities enable organizations to simulate system behavior, test proposed changes, and analyze scenarios without affecting production systems. Current IT Service Management practices lack simulation capabilities for change impact analysis. Current Information Assurance practices lack simulation capabilities for security control validation. Digital twins address these gaps by providing virtual environments synchronized with operational systems for testing and analysis.

2.13.2 Research Justification and Theoretical Contribution

The literature review establishes clear justification for this research through multiple converging factors. Digital Engineering has demonstrated value in traditional systems engineering domains. Compliance frameworks explicitly require enterprise architecture capabilities that current approaches fail to provide. Research documents pervasive failures in current IT documentation and configuration management practices. Despite these factors, academic research has not investigated Digital Engineering application to enterprise IT and Information Assurance.

This research contributes by investigating whether IT and Information Assurance professionals recognize value in Digital Engineering capabilities. If professionals perceive value, findings justify subsequent implementation research. If professionals do not perceive value despite documented challenges, findings challenge the theoretical premise and identify barriers requiring address before adoption can occur.

2.13.3 Limitations of the Theoretical Framework

The theoretical framework acknowledges several limitations. First, the framework extrapolates from Digital Engineering value demonstrated in aerospace and defense domains to anticipated value in enterprise IT contexts. Whether benefits demonstrated for physical systems transfer to logical information systems remains unvalidated. Second, the framework assumes that Digital Engineering tools and methodologies can be adapted for enterprise IT contexts. Adaptation requirements may exceed anticipated effort. Third, the framework does not address organizational change management, workforce development, or cultural transformation requirements. Adoption barriers beyond awareness and perceived value may impede implementation. Fourth, the framework focuses upon potential benefits without comprehensive analysis of costs or implementation challenges. Cost-benefit analysis requires empirical data this research does not collect.

2.14 Chapter Summary

This literature review has examined the current body of knowledge across nine interconnected domains relevant to applying Digital Engineering methodologies to Information Assurance and IT Service Management. The review established that Digital Engineering has demonstrated value in aerospace, defense, and manufacturing contexts, with authoritative guidance from organizations including the Department of Defense, NASA, and INCOSE providing mature frameworks and methodologies. Yet systematic examination across major academic databases revealed a research gap: with the sole exception of the reference model by Bonar and Hastings, no peer-reviewed research addresses Digital Engineering application to enterprise IT infrastructure, IT Service Management, or Information Assurance programs.

This gap exists despite explicit requirements within compliance frameworks for enterprise architecture capabilities that current practices demonstrably fail to provide. The section on enterprise visibility and documentation failures synthesized peer-reviewed research and industry analysis demonstrating that these challenges reflect systemic patterns: sixty-six percent visibility into IT environments, two hundred four day average breach detection times, and configuration errors causing sixty-four percent of outages. The theoretical framework developed from this synthesis posits that Digital Engineering offers disciplinary solutions to these persistent challenges.

The review examined the Unified Architecture Framework as the consolidating standard for enterprise architecture, explaining how OMG developed UAF to unify DoDAF, MODAF, NAF, and commercial frameworks with adoption by the Department of Defense, NATO, and the UK Ministry of Defence. The review analyzed Model-Based Enterprise limitations that impede enterprise IT adoption, identifying scope restrictions, organizational barriers, and skills gaps that prevent MBE practices from extending beyond manufacturing contexts. The review explored barriers to Digital Engineering adoption outside defense and aerospace, documenting platform-centric adoption patterns, organizational separation between IT and engineering functions, and economic factors that discourage investment without demonstrated return.

The review examined open source standards and tools for MBSE, digital twins, and PLM, finding that options exist but academic research validating their application to enterprise IT contexts does not. This absence of academic evidence leaves organizations without peer-reviewed guidance for adoption decisions, relying instead upon vendor claims and gray literature that may not reflect objective assessment.

Chapter 3 presents the research methodology employed to investigate professional awareness and perceptions of Digital Engineering capabilities. The methodology utilizes a quantitative survey-based approach following a systems engineering lifecycle to ensure rigor and traceability throughout the research process.

References

[1] Cybersecurity and Infrastructure Security Agency, *Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways | CISA*, Government Cybersecurity Advisory, Washington, District of Columbia, Feb. 2024. Accessed: Jan. 17, 2026. [Online]. Available: `https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b`

[2] Cybersecurity and Infrastructure Security Agency, "Emergency Directive 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," Cybersecurity and Infrastructure Security Agency, Emergency Directive, Jan. 2024. Accessed: Jan. 3, 2025. [Online]. Available: `https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities`

[3] R. Ross et al., "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, Special Publication (NIST SP) NIST SP 800-53 Rev. 5, Sep. 2020. DOI: `10.6028/NIST.SP.800-53r5` [Online]. Available: `https://csrc.nist.gov/pubs/sp/800/53/r5/final`

[4] D. Cannon, *ITIL: IT Service Management Practices. Volume 1: Service Strategy* (AXELOS - Global Best Practice), 2011 ed., 2nd impr. London, United Kingdom: TSO, The Stationery Office, 2013, ISBN: 978-0-11-331304-4.

[5] Object Management Group, "Unified Architecture Framework (UAF) Specification Version 1.2," Object Management Group, Standard ISO/IEC 19540-1:2022 and ISO/IEC 19540-2:2022, 2022. Accessed: Jan. 3, 2025. [Online]. Available: `https://www.omg.org/spec/UAF/1.2`

[6] H. Benbya, N. Nan, H. Tanriverdi, and Y. Yoo, "Complexity and Information Systems Research in the Emerging Digital World," *MIS Quarterly*, vol. 44, no. 1, pp. 1–17, 2020. DOI: `10.25300/MISQ/2020/13304` [Online]. Available: `https://misq.umn.edu/complexity-and-information-systems-research-in-the-emerging-digital-world.html`

[7] B. Bokan and J. Santos, "Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures," in *2021 Systems and Information Engineering Design Symposium (SIEDS)*, IEEE, 2021, pp. 1–6. DOI: `10.1109/SIEDS52267.2021.9483736`

[8] International Organization for Standardization, "ISO 31000:2018 Risk Management — Guidelines," International Organization for Standardization, Geneva, CH,

Standard, 2018. [Online]. Available: https://www.iso.org/standard/65694.html

[9] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, NIST Cybersecurity Framework, 2014. Accessed: Jan. 3, 2025. [Online]. Available: https://www.nist.gov/cyberframework

[10] Information Systems Audit and Control Association (ISACA), *COBIT 2019 Framework: Introduction and Methodology.* Schaumburg, IL: Information Systems Audit and Control Association, 2018, ISBN: 978-1-60420-644-9.

[11] International Organization for Standardization, "ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements," International Organization for Standardization, Standard, 2022. DOI: 10.1109/IEEESTD.2023.10123367 [Online]. Available: https://www.iso.org/standard/27001

[12] Gartner, *Why CMDB Projects Fail and How to Avoid Their Mistakes*, Gartner Research, 2019. Accessed: Jan. 3, 2025. [Online]. Available: https://www.gartner.com/en/documents/3970851

[13] IDC and Exabeam, "The State of Threat Detection, Investigation, and Response," IDC, Research Report, 2023. Accessed: Jan. 3, 2026. [Online]. Available: https://www.exabeam.com/wp-content/uploads/REPORT-Exabeam-The-State-of-TDIR-2023-NA-EN.pdf

[14] Gartner, *Shadow IT: The Risks and How to Manage Them*, Gartner Research, 2022. Accessed: Jan. 3, 2025. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/shadow-it

[15] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2024," IBM Corporation, Research Report, Jul. 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach

[16] International Council on Systems Engineering (INCOSE), *Digital Engineering Information Exchange Working Group*, Online. Accessed: Jan. 3, 2025. [Online]. Available: https://www.incose.org/communities/working-groups-initiatives/digital-engineering-information-exchange

[17] Office of the Under Secretary of Defense for Research and Engineering, *Systems Engineering Guidebook.* Department of Defense, Feb. 2022. Accessed: Jan. 3, 2025. [Online]. Available: https://ac.cto.mil/wp-content/uploads/2022/02/Systems-Eng-Guidebook_Feb2022-Cleared-slp.pdf

[18] National Aeronautics and Space Administration — Office of the Chief Engineer, "NASA Digital Engineering Acquisition Framework Handbook," National Aeronautics and Space Administration, Washington, DC, Technical Handbook NASA-HDBK-1004, Apr. 2020. [Online]. Available: https://standards.nasa.gov/standard/NASA/NASA-HDBK-1004

[19] N. Hutchison et al., *WRT-1001: Digital Engineering Metrics*. Systems Engineering Research Center, 2020. Accessed: Nov. 17, 2023. [Online]. Available: https://sercuarc.org/wp-content/uploads/2020/06/SERC-TR-2020-002-DE-Metrics-6-8-2020.pdf

[20] N. Hutchinson et al., *WRT-1006 Technical Report: Developing the Digital Engineering Competency Framework (DECF) Phase 2*. Systems Engineering Research Center, 2021. Accessed: Nov. 17, 2023. [Online]. Available: https://sercproddata.s3.us-east-2.amazonaws.com/technical_reports/reports/1616668486.A013_SERC%20WRT%201006_Technical%20Report%20SERC-2021-TR-005_FINAL.pdf

[21] L. Baker, P. Clemente, B. Cohen, L. Permenter, B. Purves, and P. Salmon, "System Architecture and Model-Based Systems Engineering for Complex Systems Governance," *Systems Engineering*, vol. 23, no. 3, pp. 345–358, 2020. DOI: 10.1002/sys.21525

[22] H. Zhang and F. Moller, "Architecture-Centric Model-Based Systems Engineering for Complex Systems," in *Proceedings of the International Conference on Software Engineering and Knowledge Engineering*, IEEE, 2021, pp. 123–130.

[23] G. Shao, *Use Case Scenarios for Digital Twin Implementation Based on ISO 23247* (NIST Advanced Manufacturing Series 400-2). National Institute of Standards and Technology, May 2021. DOI: 10.6028/NIST.AMS.400-2 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.400-2.pdf

[24] A. M. Madni and M. Sievers, "Leveraging Digital Twin Technology in Model-Based Systems Engineering," *Systems*, vol. 6, no. 1, p. 7, 2018. DOI: 10.3390/systems6010007 [Online]. Available: https://www.mdpi.com/2079-8954/6/1/7

[25] L. U. Khan, W. Saad, D. Niyato, Z. Han, and C. S. Hong, "Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions," *IEEE Communications Magazine*, vol. 60, no. 1, pp. 74–80, 2022. DOI: 10.1109/MCOM.001.21143

[26] R. Ross, M. Winstead, and M. McEvilley, *Engineering Trustworthy Secure Systems* (NIST Special Publication 800-160 Vol. 1 Rev. 1). National Institute of Standards and Technology, Nov. 2022. DOI: 10.6028/NIST.SP.800-160v1r1 [Online]. Available: https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

[27] Department of Defense, "Digital Engineering Strategy," Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Strategic Document, Jun. 2018. Accessed: Jan. 3, 2025. [Online]. Available: https://ac.cto.mil/digital_engineering/

[28] National Aeronautics and Space Administration, "Future Model-Based Systems Engineering Vision and Strategy Bridge for NASA," NASA, Technical Memorandum NASA/TM-20210014025, 2021. Accessed: Jan. 3, 2025. [Online]. Available: https://ntrs.nasa.gov/citations/20210014025

[29] J. Bonar and J. Hastings, "Transforming Information Systems Management: A Reference Model for Digital Engineering Integration," in *2024 Cyber Awareness and Research Symposium (CARS)*, IEEE, 2024, pp. 1–9. DOI: 10.1109/CARS61786.2024.10778791

[30] Object Management Group, *About the Unified Architecture Framework Specification*, Online, 2024. Accessed: Jan. 3, 2025. [Online]. Available: https://www.omg.org/spec/UAF/About-UAF/

[31] Object Management Group, "Unified Architecture Framework (UAF) Domain Metamodel Version 1.2," Object Management Group, Specification, 2022. Accessed: Jan. 3, 2025. [Online]. Available: https://www.omg.org/spec/UAF/1.2/DMM

[32] The Aerospace Corporation, *Unified Architecture Framework (UAF)*, Online, 2023. Accessed: Jan. 3, 2025. [Online]. Available: https://aerospace.org/story/unified-architecture-framework-uaf

[33] J. Bankauskaite, "Enterprise Architecture Frameworks Analysis," in *CEUR Workshop Proceedings*, vol. 2470, 2019, pp. 141–149. Accessed: Jan. 3, 2025. [Online]. Available: https://ceur-ws.org/Vol-2470/p19.pdf

[34] National Defense Industrial Association Systems Engineering Division, "Evaluation of DoDAF Meta-model Support for Systems Engineering," National Defense Industrial Association, Technical Report, 2011.

[35] M. Hause, G. Bleakley, and A. Morkevicius, "Technology Update on the Unified Architecture Framework (UAF)," Object Management Group, Conference Paper, 2017. DOI: 10.1002/j.2334-5837.2015.00066.x

[36] NATO, "NATO Architecture Framework Version 4," North Atlantic Treaty Organization, Architecture Framework, 2018. Accessed: Jan. 3, 2025. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_157575.htm

[37] Department of Defense, "DoD Architecture Framework Version 2.02," Department of Defense, Chief Information Officer, Framework Document, 2009. Accessed:

Jan. 3, 2025. [Online]. Available: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/

[38] Defense Acquisition University, *DoD Architecture Framework (DoDAF)*, Acquipedia, 2024. Accessed: Jan. 3, 2025. [Online]. Available: https://www.dau.edu/acquipedia-article/dod-architecture-framework-dodaf

[39] M. Hause, "Evaluation of the DoDAF Meta-model's Support of Systems Engineering," in *Procedia Computer Science*, vol. 61, Elsevier, 2015, pp. 254–260. DOI: 10.1016/j.procs.2015.09.208 [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915030380

[40] The Open Group, *TOGAF Standard, Version 9.2*. Reading, UK: The Open Group, 2018, ISBN: 978-9401802833. Accessed: Jun. 3, 2023. [Online]. Available: https://www.opengroup.org/togaf

[41] The Open Group and MITRE Corporation, "Using TOGAF to Define and Govern Service-Oriented Architectures," The Open Group, White Paper, 2013. [Online]. Available: https://www.opengroup.org/togaf

[42] J. A. Zachman, "The Concise Definition of the Zachman Framework," *Zachman International*, 2008. Accessed: Jan. 3, 2026. [Online]. Available: https://www.zachman.com/about-the-zachman-framework

[43] J. A. Zachman, "The Zachman Framework Evolution," *Zachman International Enterprise Architecture*, 2011. Accessed: Jan. 3, 2025. [Online]. Available: https://www.zachman.com

[44] R. Eichmann, S. Melzer, and R. God, "Model-based Development of a System of Systems Using Unified Architecture Framework (UAF): A Case Study," in *2019 IEEE International Systems Conference (SysCon)*, IEEE, 2019, pp. 1–6. DOI: 10.1109/SYSCON.2019.8836749 [Online]. Available: https://ieeexplore.ieee.org/document/8836749

[45] A. Abhaya, "UAF (Unified Architecture Framework) Based MBSE (UBM) Method to Build a System of Systems Model," *INCOSE International Symposium*, vol. 31, no. 1, pp. 515–530, 2021. DOI: 10.1002/j.2334-5837.2021.00835.x [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2021.00835.x

[46] Z. Liu et al., "Top-Down Military System-of-Systems Design Using MBSE Based on UAF: A Case Study," in *Advances in Guidance, Navigation and Control*, Springer, 2023, pp. 203–214. DOI: 10.1007/978-981-99-6511-3_19 [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-99-6511-3_19

[47] M. Torkjazi et al., “Model-Based Systems Engineering (MBSE) Methodology for Integrating Autonomy into a System of Systems Using the Unified Architecture Framework,” *INCOSE International Symposium*, vol. 34, no. 1, pp. 726–742, 2024. DOI: `10.1002/iis2.13195` [Online]. Available: `https://incose.onlinelibrary.wiley.com/doi/10.1002/iis2.13195`

[48] Department of Defense, “DoD Instruction 5000.97: Digital Engineering,” Department of Defense, Instruction, Dec. 2023. Accessed: Jan. 3, 2025. [Online]. Available: `https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500097p.pdf`

[49] National Aeronautics and Space Administration, “NASA Digital Engineering Acquisition Framework Handbook,” NASA, Handbook NASA-HDBK-1004, Apr. 2020. Accessed: Jan. 3, 2025. [Online]. Available: `https://standards.nasa.gov/standard/NASA/NASA-HDBK-1004`

[50] International Council on Systems Engineering, *Systems Engineering Vision 2035*. International Council on Systems Engineering, 2021. Accessed: Jan. 3, 2025. [Online]. Available: `https://www.incose.org/about-systems-engineering/se-vision-2035`

[51] International Council on Systems Engineering, *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, 5th. Wiley, 2023, ISBN: 978-1119814290. DOI: `10.1002/9781119814436`

[52] SEBoK Authors, *The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.13*, N. Hutchison, Ed., www.sebokwiki.org, 2025.

[53] National Institute of Standards and Technology, “Framework for Cyber-Physical Systems: Volume 1, Overview,” NIST, Special Publication NIST SP 1500-201, 2017. DOI: `10.6028/NIST.SP.1500-201` [Online]. Available: `https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview`

[54] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, “Developing Cyber-Resilient Systems: A Systems Security Engineering Approach,” National Institute of Standards and Technology, Special Publication 800-160 Vol. 2 Rev. 1, Dec. 2021. DOI: `10.6028/NIST.SP.800-160v2r1` [Online]. Available: `https://csrc.nist.gov/publications/detail/sp/800-160/vol-2-rev-1/final`

[55] M. Helu and T. Hedberg, “Security and Trust Considerations for Digital Twin Technology,” National Institute of Standards and Technology, Internal Report NIST IR 8356, 2025. DOI: `10.6028/NIST.IR.8356` [Online]. Available: `https://csrc.nist.gov/pubs/ir/8356/final`

[56] G. Shao, S. Frechette, and V. Srinivasan, "An Analysis of the New ISO 23247 Series of Standards on Digital Twin Framework for Manufacturing," in *ASME 2023 18th International Manufacturing Science and Engineering Conference*, ASME, 2023. DOI: 10.1115/MSEC2023-101127 [Online]. Available: https://www.nist.gov/publications/analysis-new-iso-23247-series-standards-digital-twin-framework-manufacturing

[57] Systems Engineering Research Center, "Enterprise System-of-Systems Model for Digital Thread Enabled Acquisition," SERC, Technical Report SERC-2018-TR-109, 2018. [Online]. Available: https://sercuarc.org/technical-reports/

[58] Systems Engineering Research Center, "Systems Engineering Modernization: Digital Engineering, MOSA, Mission Engineering, and Agile/DevOps Integration," SERC, Technical Report SERC-2022-TR-009, 2022. [Online]. Available: https://www.cto.mil/wp-content/uploads/2023/06/SERC-WRT-1051-2023.pdf

[59] A. Wooley and J. Womack, "Digital Engineering: A Systematic Literature Review of Strategies, Components, and Implementation Challenges," *Systems*, vol. 13, no. 12, p. 1046, 2025. DOI: 10.3390/systems13121046

[60] K. Henderson and A. Salado, "Value and Benefits of Model-Based Systems Engineering (MBSE): Evidence from the Literature," *Systems Engineering*, vol. 24, no. 1, pp. 51–66, 2021. DOI: 10.1002/sys.21566 Accessed: Aug. 3, 2025. [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/10.1002/sys.21566

[61] S. Wolny, A. Mazak, C. Carpella, V. Geist, and M. Wimmer, "Thirteen Years of SysML: A Systematic Mapping Study," *Software and Systems Modeling*, vol. 19, no. 1, pp. 111–169, 2020. DOI: 10.1007/s10270-019-00735-y Accessed: Feb. 17, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10270-019-00735-y

[62] M. Chami and J.-M. Bruel, "A Survey on Model-Based Systems Engineering: Challenges and Perceptions," in *Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development*, SCITEPRESS, 2018, pp. 213–220. DOI: 10.5220/0006607802130220 [Online]. Available: https://hal.science/hal-02124402v1/document

[63] J. Gregory, L. Berthoud, T. Tryfonas, and A. Sherlock, "Model Based Engineering (MBE): An Examination of Current Practice in UK Defence," in *INCOSE International Symposium*, vol. 29, 2019, pp. 614–628. DOI: 10.1002/j.2334-5837.2019.00623.x

[64] S. Friedenthal, A. Moore, and R. Steiner, *A Practical Guide to SysML: The Systems Modeling Language*, 3rd. Morgan Kaufmann, 2014, ISBN: 978-0128002025.

[65] M. Grieves, “Digital Twin: Manufacturing Excellence through Virtual Factory Replication,” *Digital Twin*, vol. 3, pp. 1–35, 2023. DOI: 10.12688/digitaltwin.17469.2

[66] M. Eckhart and A. Ekelhart, “Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook,” in *Security and Quality in Cyber-Physical Systems Engineering*, Springer, 2019, pp. 383–412. DOI: 10.1007/978-3-030-25312-7_14 [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-25312-7_14

[67] E. Karaarslan and M. Babiker, “Digital Twin Security Threats and Countermeasures: An Introduction,” in *2021 International Conference on Information Security and Cryptology (ISCTURKEY)*, IEEE, 2021, pp. 7–11. DOI: 10.1109/ISCTURKEY53027.2021.9654360

[68] M. Vielberth, M. Dietz, D. Gollmann, and G. Pernul, “A Digital Twin-Based Cyber Range for SOC Analysts,” in *Data and Applications Security and Privacy XXXV*, Springer, 2021, pp. 293–311. DOI: 10.1007/978-3-030-81242-3_17 [Online]. Available: https://dl.acm.org/doi/10.1007/978-3-030-81242-3_17

[69] M. Dietz and G. Pernul, “Digital Twin: Empowering Enterprises Towards a System-of-Systems Approach,” *IEEE Security & Privacy*, vol. 18, no. 5, pp. 46–53, 2020. DOI: 10.1109/MSEC.2020.2983348

[70] J. Campagna, E. Markopoulos, and A. Soylu, “Strategic Adoption of Digital Innovations Leading to Digital Transformation: A Literature Review and Discussion,” *Systems*, vol. 12, no. 4, p. 118, 2024. DOI: 10.3390/systems12040118

[71] Eclipse Foundation, *Papyrus: Open Source UML and SysML Modeling Environment*, Online, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://eclipse.dev/papyrus/

[72] Eclipse Foundation, *Capella: Open Source MBSE Tool*, Online, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://mbse-capella.org/

[73] Obeo, *SysON: The NextGen SysML Modeling Tool*, Online, 2025. Accessed: Jan. 9, 2025. [Online]. Available: https://mbse-syson.org/

[74] Digital Twin Consortium, *Digital Twin Open-Source Collaboration Initiative*, GitHub Repository, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://www.digitaltwinconsortium.org/initiatives/open-source/

[75] Eclipse Foundation, *Eclipse Ditto: Open Source Framework for Digital Twins in the IoT*, Online, 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://eclipse.dev/ditto/

[76] Eclipse Foundation, *Eclipse BaSyx: Open Source Industry 4.0 Middleware*, Online, 2024. Accessed: Jan. 9, 2025. [Online]. Available: `https://eclipse.dev/basyx/`

[77] S. Gil, C. Martín, and M. Díaz, "Survey on Open-Source Digital Twin Frameworks: A Case Study Approach," *Software: Practice and Experience*, vol. 54, no. 1, pp. 108–145, 2024. DOI: `10.1002/spe.3305`

[78] J. Autiosalo, J. Siegel, and K. Tammi, "Twinbase: Open-Source Server Software for the Digital Twin Web," *IEEE Access*, vol. 9, pp. 140 779–140 798, 2021. DOI: `10.1109/ACCESS.2021.3119487`

[79] O. Grabov, *The Future of Open Source in PLM: Can It Solve Key Problems?* Beyond PLM Blog, 2024. Accessed: Jan. 9, 2025. [Online]. Available: `https://beyondplm.com/2024/09/23/the-future-of-open-source-in-plm-can-it-solve-key-problems/`

[80] M. Laili, S. Pekkola, and J. Kääriäinen, "Industrial Open Source Solutions for Product Life Cycle Management," *Cogent Engineering*, vol. 1, no. 1, p. 939 737, 2014. DOI: `10.1080/23311916.2014.939737`

[81] Joint Task Force Transformation Initiative, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," National Institute of Standards and Technology, Special Publication NIST Special Publication (SP) 800-37, Rev. 2, Dec. 2018. DOI: `10.6028/NIST.SP.800-37r2`

[82] Committee on National Security Systems, "Security Categorization and Control Selection for National Security Systems," CNSS, Instruction CNSSI 1253, 2022. [Online]. Available: `https://www.cnss.gov/CNSS/issuances/Instructions.cfm`

[83] National Institute of Standards and Technology, "Open Security Controls Assessment Language (OSCAL)," NIST, Technical Specification, 2023. Accessed: Jan. 3, 2025. [Online]. Available: `https://pages.nist.gov/OSCAL/`

[84] AXELOS Limited, *ITIL Foundation: ITIL 4th Edition.* Norwich, UK: The Stationery Office (TSO), 2019, Official ITIL 4 Guidance, ISBN: 9780113316076.

[85] Gartner, *CMDB Data Quality: Critical Success Factors*, Gartner Research, 2020. Accessed: Jan. 3, 2025. [Online]. Available: `https://www.gartner.com/en/information-technology/glossary/cmdb-configuration-management-database`

[86] Forrester Research, *The State of Configuration Management*, Forrester Research Report, 2020.

[87] IBM, *The Cost of Poor Data Quality*, IBM Research, 2020. Accessed: Jan. 17, 2026. [Online]. Available: https://www.ibm.com/thought-leadership/institute-business-value/

[88] C. Betz, "CMDB Is Dead—Long Live The IT Management Graph," Oct. 2025. Accessed: Jan. 9, 2025. [Online]. Available: https://www.forrester.com/blogs/cmdb-is-dead-long-live-the-it-management-graph/

[89] L. S. Cook, G. E. Gann, K. V. Ray, and X. Zhang, "IT Service Management Implementation Challenges: A Review," *Issues in Information Systems*, vol. 22, no. 2, pp. 196–208, 2021. DOI: 10.48009/2_iis_2021_196-208 [Online]. Available: https://www.iacis.org/iis/2021/2_iis_2021_196-208.pdf

[90] M. Marrone and L. M. Kolbe, "Impact of IT Service Management Frameworks on the IT Organization," *Business & Information Systems Engineering*, vol. 3, no. 1, pp. 5–18, 2011. DOI: 10.1007/s12599-010-0141-5 [Online]. Available: https://link.springer.com/article/10.1007/s12599-010-0141-5

[91] Freshworks, *Change Management Best Practices*, Online, Nov. 2025. Accessed: Jan. 3, 2025. [Online]. Available: https://www.freshworks.com/change-management/best-practices/

[92] International Organization for Standardization, "Information technology - Service management - Part 1: Service management system requirements," International Organization for Standardization, Geneva, CH, Standard ISO/IEC 20000-1:2018, Sep. 2018.

[93] H. Thompson, M. Anderson, and S. Johnson, "Integrating mbse with it service management: A practical approach," *Journal of Enterprise Architecture*, vol. 15, no. 3, pp. 42–55, Aug. 2019, ISSN: 1556-9365.

[94] Ponemon Institute, "Global Study on Closing the IT Security Gap," Ponemon Institute, Research Report, 2023. Accessed: Jan. 9, 2025. [Online]. Available: https://ponemonsullivanreport.com/2023/07/closing-the-it-security-gap-what-are-high-performers-doing-differently/

[95] SANS Institute, "SOC Survey 2023," SANS Institute, Research Report, 2023. Accessed: Jan. 9, 2025. [Online]. Available: https://www.sans.org/white-papers/

[96] Ivanti, "State of Cybersecurity Trends Report 2025," Ivanti, Research Report, 2025. Accessed: Jan. 9, 2025. [Online]. Available: https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report

[97] Cloud Security Alliance, “Cloud Security Study 2024,” Cloud Security Alliance, Research Report, Jul. 2024. Accessed: Jan. 9, 2025. [Online]. Available: https://cloudsecurityalliance.org/research/

[98] Check Point Software Technologies and Cybersecurity Insiders, “2024 cloud security report: Navigating the intersection of cybersecurity and ai,” Check Point Software Technologies Ltd., Tech. Rep., May 2024. Accessed: Jan. 2, 2026. [Online]. Available: https://engage.checkpoint.com

[99] M. Hauder, F. Matthes, and S. Roth, “Challenges for Automated Enterprise Architecture Documentation,” in *Lecture Notes in Business Information Processing*, vol. 131, Springer, 2012, pp. 21–39. DOI: 10.1007/978-3-642-34163-2_2

[100] Z. Yin, X. Yuan, Y. Lu, et al., “An Empirical Study on Configuration Errors in Commercial and Open Source Systems,” in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, ser. SOSP ’11, ACM, 2011, pp. 159–172. DOI: 10.1145/2043556.2043572

[101] National Institute of Standards and Technology, “Guide for Security-Focused Configuration Management of Information Systems,” National Institute of Standards and Technology, Special Publication 800-128, 2019. DOI: 10.6028/NIST.SP.800-128 [Online]. Available: https://csrc.nist.gov/pubs/sp/800/128/final

[102] Uptime Institute, “Annual Outage Analysis 2023,” Uptime Institute, Research Report, 2023. Accessed: Jan. 3, 2026. [Online]. Available: https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[103] IT Process Institute, “The Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps,” IT Process Institute, Handbook, 2004.

[104] IBM Security and Ponemon Institute, “Cost of a Data Breach Report 2025,” IBM Corporation, Research Report, 2025. Accessed: Jan. 9, 2025. [Online]. Available: https://www.ibm.com/reports/data-breach

[105] F. Bento, M. Tagliabue, and F. Lorenzo, “Organizational Silos: A Scoping Review Informed by a Behavioral Perspective on Systems and Networks,” *Societies*, vol. 10, no. 3, p. 56, 2020. DOI: 10.3390/soc10030056

[106] T. Brée and E. Karger, “Challenges in Enterprise Architecture Management: Overview and Future Research,” *Journal of Governance and Regulation*, vol. 11, no. 2, pp. 8–21, 2022. DOI: 10.22495/jgrv11i2art1

[107] H. Benbya and B. McKelvey, “Toward a Complexity Theory of Information Systems Development,” *Information Technology & People*, vol. 19, no. 1, pp. 12–34, 2006. DOI: 10.1108/09593840610649952

[108] G. Santos et al., "Documentation Technical Debt," in *Proceedings of the XXXIII Brazilian Symposium on Software Engineering*, ser. SBES '19, ACM, 2019, pp. 304–313. DOI: 10.1145/3350768.3350773

[109] Z. Li, P. Avgeriou, and P. Liang, "A Systematic Mapping Study on Technical Debt and Its Management," *Journal of Systems and Software*, vol. 101, pp. 193–220, 2015. DOI: 10.1016/j.jss.2014.12.027

[110] N. S. A. Junior and G. H. Travassos, "Consolidating a Common Perspective on Technical Debt and Its Management through a Tertiary Study," *Information and Software Technology*, vol. 150, p. 106 991, 2022. DOI: 10.1016/j.infsof.2022.106991

[111] Z. Kleinwaks, "Technical Debt in Systems Engineering: A Systematic Literature Review," *Systems Engineering*, vol. 26, no. 6, pp. 710–726, 2023. DOI: 10.1002/sys.21681

[112] Forrester Research, "It's Go Time For Application And Infrastructure Dependency Mapping (AIDM)," Forrester Research, Research Report RES141653, 2018. Accessed: Jan. 9, 2025. [Online]. Available: https://www.forrester.com/report/Its-Go-Time-For-Application-And-Infrastructure-Dependency-Mapping-AIDM/RES141653

[113] Cisco Systems, Inc., *You can't manage what you can't see: Cisco helps businesses address shadow IT*, Cisco Investor Relations, Jan. 2016. Accessed: Jan. 17, 2026. [Online]. Available: https://investor.cisco.com/news/news-details/2016/You-Cant-Manage-What-You-Cant-See-Cisco-Helps-Businesses-Address-Shadow-IT/default.aspx

[114] Gartner, *Top Threats to Cloud Computing and Security Trends 2024*, Gartner Research, 2024. Accessed: Dec. 21, 2025. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

[115] A. A. Hassan and W. M. Bahgat, "A Framework for Translating a High Level Security Policy into Low Level Security Mechanisms," in *2009 IEEE/ACS International Conference on Computer Systems and Applications*, IEEE, May 2009, pp. 504–511. DOI: 10.1109/AICCSA.2009.5069371

[116] L. Apvrille and Y. Roudier, "SysML-Sec: A Model Driven Approach for Designing Safe and Secure Systems," in *2015 3rd International Conference on Model-Driven Engineering and Software Development (MODELSWARD)*, IEEE, 2015, pp. 655–664. DOI: 10.5220/0005402006550664