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 12, 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

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 technology, 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.

The investigation pursues three research questions. First, to what extent do IT and information assurance professionals possess awareness of Digital Engineering capabilities? Second, do these practitioners perceive such capabilities as valuable for their work in security compliance, threat mitigation, and service delivery? Third, do they believe Digital Engineering practices would enhance their ability to execute their duties, satisfy regulatory mandates, or strengthen organizational posture? These questions address an unresolved gap between proven systems engineering methods and the persistent documentation failures, visibility deficiencies, and traceability shortfalls that characterize contemporary IT and information assurance operations.

This research targets IT and information assurance professionals across defense, government, commercial, healthcare, education, and non-profit sectors, enabling assessment of whether Digital Engineering awareness and perceived value vary by organizational context. The benefits demonstrated in defense and aerospace—reduced development timelines, improved configuration management, enhanced compliance verification—suggest logical application to organizations outside these sectors, including resource-constrained entities serving underrepresented populations.

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.

TABLE OF CONTENTS

Abstract . . . . . **ii**

Table of Contents . . . . . **iii**

List of Tables . . . . . **vii**

List of Figures . . . . . **viii**

Chapter 1:

Introduction **1**

1.1 Current State of Information System Management 3

1.1.1 Information Assurance Practice 4

1.1.2 IT Service Management Practice 6

1.1.3 Challenges in Current Practice 7

1.2 Digital Engineering as Potential Solution 9

1.2.1 Model-Based Systems Engineering 10

1.2.2 Digital Threads 12

1.2.3 Digital Twin 13

1.2.4 Product Lifecycle Management 14

1.3 Gaps in Current Practice 16

1.3.1 Information Assurance Challenges 16

1.3.2 IT Service Management Challenges 17

1.3.3 The Documentation-Reality Gap 18

1.4 Research Questions . . . 19
1.5 Research Scope and Approach . . . 20
1.5.1 Methodological Approach . . . 20
1.5.2 Target Population and Broader Application . . . 21
1.5.3 Potential Benefits for Organizations Serving Underrepresented Populations . . . 22
1.5.4 Why Perceptions Matter . . . 24
1.5.5 Contribution of Prior Research . . . 24
1.6 Significance of the Research . . . 25
1.6.1 Academic Significance . . . 25
1.6.2 Industry Significance . . . 26
1.6.3 Commonwealth Significance . . . 26
1.6.4 Societal Significance . . . 27
1.7 Chapter Summary . . . 28

References . . . 30

Appendix A: Survey Question to Research Question Mapping . . . 34
A.1 Research Questions . . . 34
A.2 Survey Structure Aligned to Core Dimensions . . . 35
A.3 Section 1: Awareness and Familiarity with Digital Engineering . . . 36
A.3.1 Core Dimension: Awareness . . . 36
A.3.2 Primary Research Question — RQ1 . . . 36
A.3.3 Rationale . . . 36
A.4 Section 2: Understanding of Digital Engineering Capabilities . . . 37
A.4.1 Core Dimension: Awareness . . . 37
A.4.2 Primary Research Question — RQ1 . . . 37
A.4.3 Rationale . . . 37

A.5 Section 3: Applicability of Digital Engineering 38
A.5.1 Core Dimension: Applicability 38
A.5.2 Primary Research Questions — RQ2, RQ3 38
A.5.3 Rationale 39
A.6 Section 4: Value Assessment for Information Technology 40
A.6.1 Core Dimension Perceived Value (IT Domain) 40
A.6.2 Primary Research Questions — RQ2, RQ3 40
A.6.3 Rationale 40
A.7 Section 5: Value Assessment for Information Assurance 42
A.7.1 Core Dimension: Perceived Value (Information Assurance Domain) 42
A.7.2 Primary Research Questions — RQ2, RQ3 42
A.7.3 Rationale 43
A.8 Section 6: Interest and Demographic Information 43
A.8.1 Core Dimension: Supporting/Demographics 43
A.8.2 Rationale 44
A.9 Summary: Question Distribution by Research Question 44
A.10 Summary: Question Distribution by DE Pillar 45
A.11 Analysis Framework 45
A.11.1 Primary Analysis for Each Research Question 45
A.11.2 Composite Scores 46
A.12 Scale Reference 47
A.12.1 Familiarity Scale (Q1.1) 47
A.12.2 Agreement Scale (Q2.1-Q5.6) 47
A.12.3 Experience Level Categories (Q6.4) 47

Appendix B: Artificial Intelligence Assistance Disclosure 48

B.1 AI Tools Utilized 48
B.2 Scope of AI Assistance 48

B.3 Scope Limitations 49
B.4 Author Responsibility 49
B.5 Rationale for Disclosure 50

LIST OF TABLES

Table A.1 Research Questions 34

Table A.2 Survey Section Structure 35

Table A.3 Section 1 Question Mapping 36

Table A.4 Section 2 Question Mapping 37

Table A.5 Section 3 Question Mapping 38

Table A.6 Section 4 Question Mapping 40

Table A.7 Section 5 Question Mapping 42

Table A.8 Section 6 Question Mapping 43

Table A.9 Question Distribution by Research Question 44

Table A.10 Question Distribution by Digital Engineering Pillar 45

Table A.11 Composite Score Definitions 46

Table A.12 Familiarity Scale 47

Table A.13 Agreement Scale 47

Table A.14 Experience Level Categories 47

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 ex-

tended 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 automat-

ically 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 ap-

proaches 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 assur-

ance 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.

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

Appendix A

Survey Question to Research Question Mapping

This appendix provides traceability between survey questions and research questions, following the systems engineering lifecycle approach outlined in the dissertation methodology. The survey structure addresses three core dimensions—**Awareness**, **Applicability**, and **Perceived Value**—as they pertain to Digital Engineering and its four pillars: Model-Based Systems Engineering, the Digital Thread, Digital Twin, and Product Lifecycle Management.

A.1 Research Questions

Table A.1: Research Questions

RQ	Research Question
RQ1	To what extent are IT and information assurance professionals aware of Digital Engineering capabilities, including MBSE, the Digital Thread, digital twin technologies, and PLM principles?
RQ2	Do IT and information assurance professionals perceive Digital Engineering capabilities as potentially valuable or important for their work in IA, security compliance, and IT service delivery?
RQ3	Do IT and information assurance professionals believe DE practices would help them perform their jobs, meet compliance requirements, or enhance organizational capabilities?

A.2 Survey Structure Aligned to Core Dimensions

Table A.2: Survey Section Structure

Section	Core Dimension	Primary RQ	Description
Section 1	Awareness	RQ1	Baseline familiarity and professional exposure
Section 2	Awareness	RQ1	Understanding of specific DE capabilities/pillars
Section 3	Applicability	RQ2, RQ3	Perceived relevance to IT and IA domains
Section 4	Perceived Value	RQ2, RQ3	Value assessment for IT operations
Section 5	Perceived Value	RQ2, RQ3	Value assessment for IA/Cybersecurity operations
Section 6	Demographics	Supporting	Professional field and experience level

A.3 Section 1: Awareness and Familiarity with Digital Engineering

A.3.1 Core Dimension: Awareness

A.3.2 Primary Research Question — RQ1

Table A.3: Section 1 Question Mapping

Q#	Question Text	Format	DE Pillar	RQ
1.1	Please rate your level of familiarity with Digital Engineering concepts and practices.	5-point Likert (Familiarity)	All/General	RQ1
1.2	Have you encountered Digital Engineering methodologies, frameworks, or tools in your professional work within the past two years?	Binary (Yes/No)	All/General	RQ1

A.3.3 Rationale

These questions establish baseline awareness metrics essential to all subsequent analysis. Question 1.1 measures self-assessed familiarity (theoretical awareness), while Question 1.2 measures practical professional exposure (applied awareness). Together they distinguish between those who have merely heard of Digital Engineering and those who have encountered it in the course of their professional duties.

A.4 Section 2: Understanding of Digital Engineering Capabilities

A.4.1 Core Dimension: Awareness

A.4.2 Primary Research Question — RQ1

Table A.4: Section 2 Question Mapping

Q#	Question Text	Format	DE Pillar	RQ
2.1	DE includes model-based systems engineering approaches that can improve development processes.	5-point Likert (Agreement)	MBSE	RQ1
2.2	DE can enable digital twin development and virtual prototyping for IT systems.	5-point Likert (Agreement)	Digital Twin	RQ1
2.3	DE supports continuous integration and data-driven decision-making in technology development.	5-point Likert (Agreement)	Digital Thread	RQ1
2.4	DE enables digital twin technology that can simulate security scenarios and test defensive measures without impacting production systems.	5-point Likert (Agreement)	Digital Twin (Security)	RQ1
2.5	DE supports continuous security validation and data-driven threat analysis throughout the development lifecycle.	5-point Likert (Agreement)	Digital Thread (Security)	RQ1
2.6	DE can improve security control implementation through automated compliance checking and verification.	5-point Likert (Agreement)	PLM / Traceability	RQ1

A.4.3 Rationale

This section probes understanding of specific Digital Engineering pillars applied to IT and security contexts. Questions address all four pillars: MBSE (Q2.1), Digital Twin (Q2.2, Q2.4), the Digital Thread (Q2.3, Q2.5), and PLM with its authoritative traceability capabilities (Q2.6). The inclusion of both general IT applications (Q2.1-Q2.3) and

security-specific applications (Q2.4-Q2.6) enables meaningful comparison across professional domains.

A.5 Section 3: Applicability of Digital Engineering

A.5.1 Core Dimension: Applicability

A.5.2 Primary Research Questions — RQ2, RQ3

Table A.5: Section 3 Question Mapping

Q#	Question Text	Format	DE Pillar	RQ
3.1	DE methodologies have relevant applications within the information technology sector.	5-point Likert (Agreement)	All/General	RQ2
3.2	DE methodologies have relevant applications for addressing information assurance challenges.	5-point Likert (Agreement)	All/General	RQ2
3.3	The ability to utilize digital twins to test changes against accurate replicas of production environments would provide value to my organization.	5-point Likert (Agreement)	Digital Twin	RQ2, RQ3
3.4	The use of digital models to map and document an organization's environment and configurations would provide value to my organization.	5-point Likert (Agreement)	MBSE	RQ2, RQ3
3.5	The use of digital lifecycle management to meet compliance and service delivery requirements would provide value to my organization.	5-point Likert (Agreement)	PLM	RQ2, RQ3
3.6	My organization faces regulatory or compliance requirements that could benefit from Digital Engineering approaches.	5-point Likert (Agreement)	All/General	RQ2, RQ3

A.5.3 Rationale

This section bridges awareness and value by examining whether respondents perceive Digital Engineering as applicable to their professional contexts. Questions 3.1 and 3.2 assess domain-level applicability (IT versus IA), while Questions 3.3 through 3.5 assess pillar-specific organizational value (Digital Twin, MBSE, PLM). Question 3.6 identifies compliance-driven need, which stands central to the research focus upon Information Assurance and regulatory compliance.

A.6 Section 4: Value Assessment for Information Technology

A.6.1 Core Dimension Perceived Value (IT Domain)

A.6.2 Primary Research Questions — RQ2, RQ3

Table A.6: Section 4 Question Mapping

Q#	Question Text	Format	Value Category	RQ
4.1	DE could deliver meaningful value to my organization's information technology processes.	5-point Likert (Agreement)	Overall IT Value	RQ2, RQ3
4.2	DE could reduce development cycle time in my organization.	5-point Likert (Agreement)	Efficiency Benefit	RQ3
4.3	DE could improve product quality and reduce defects in my organization.	5-point Likert (Agreement)	Quality Benefit	RQ3
4.4	DE could improve collaboration effectiveness across development teams in my organization.	5-point Likert (Agreement)	Collaboration Benefit	RQ3
4.5	My organization would be willing to invest in DE capabilities if clear ROI could be demonstrated.	Ternary (Yes/No/ Unsure)	Investment Willingness	RQ2

A.6.3 Rationale

This section measures IT-specific value perceptions. Question 4.1 provides an overall IT value assessment. Questions 4.2 through 4.4 examine specific operational benefits—efficiency, quality, and collaboration—that directly relate to job performance as addressed by RQ3. Question 4.5 measures organizational adoption interest, indicating whether

perceived value rises to a level sufficient to warrant investment.

A.7 Section 5: Value Assessment for Information Assurance

A.7.1 Core Dimension: Perceived Value (Information Assurance Domain)

A.7.2 Primary Research Questions — RQ2, RQ3

Table A.7: Section 5 Question Mapping

Q#	Question Text	Format	Value Category	RQ
5.1	DE could deliver meaningful value to my organization's information assurance and security operations.	5-point Likert (Agreement)	Overall Security Value	RQ2, RQ3
5.2	DE could reduce the time required to identify and remediate security vulnerabilities in my organization.	5-point Likert (Agreement)	Vulnerability Mgmt Benefit	RQ3
5.3	DE could improve security posture and reduce successful cyber incidents in my organization.	5-point Likert (Agreement)	Security Posture Benefit	RQ3
5.4	DE could enhance threat modeling and risk assessment capabilities in my organization.	5-point Likert (Agreement)	Threat Modeling Benefit	RQ3
5.5	DE could improve collaboration between security teams, development teams, and operations teams in my organization.	5-point Likert (Agreement)	Cross-Team Collaboration	RQ3
5.6	DE could help my organization achieve better compliance with security frameworks and regulatory requirements.	5-point Likert (Agreement)	Compliance Benefit	RQ3
5.7	My organization would be willing to invest in DE capabilities for information assurance purposes if clear ROI could be demonstrated.	Binary (Yes/No)	Investment Willingness	RQ2

A.7.3 Rationale

This section measures information assurance-specific value perceptions. Question 5.1 provides an overall security value assessment. Questions 5.2 through 5.6 examine specific security operational benefits directly related to job performance and compliance requirements as addressed by RQ3. The emphasis upon compliance (Q5.6) directly addresses the dissertation's focus upon Information Assurance compliance frameworks. Question 5.7 measures security-specific investment willingness.

A.8 Section 6: Interest and Demographic Information

A.8.1 Core Dimension: Supporting/Demographics

A.8.1.1 Purpose

Enable subgroup analysis and assess future research/adoption interest

Table A.8: Section 6 Question Mapping

Q#	Question Text	Format	Category	RQ
6.1	Would you be interested in learning more about DE applications for information assurance and security operations in your industry?	Binary (Yes/No)	Learning Interest	Supporting
6.2	Would you recommend that your organization explore DE adoption for improving security operations?	Binary (Yes/No)	Recommendation	Supporting
6.3	Please identify your field of practice.	Categorical (IT/Security/ Engineering/Other)	Professional Field	Demographics
6.4	Please indicate your level of experience in your field of practice.	Categorical (Experience ranges)	Experience Level	Demographics

A.8.2 Rationale

Questions 6.1 and 6.2 measure forward-looking interest that complements value perception, indicating whether positive perceptions translate into desire for learning and willingness to recommend organizational exploration. Questions 6.3 and 6.4 enable comparative analysis between IT and security professionals and across experience levels, addressing whether awareness and perceptions vary systematically by professional background.

A.9 Summary: Question Distribution by Research Question

Table A.9: Question Distribution by Research Question

Research Question	**Primary Questions**	**Supporting Questions**	**Total**
RQ1 (Awareness)	Q1.1, Q1.2, Q2.1-Q2.6	—	8
RQ2 (Perceived Value)	Q3.1, Q3.2, Q3.6, Q4.1, Q4.5, Q5.1, Q5.7	Q6.1, Q6.2	7 (+2)
RQ3 (Job/Compliance Help)	Q3.3-Q3.6, Q4.1-Q4.4, Q5.1-Q5.6	—	14
Demographics	Q6.3, Q6.4	—	2

Note: Several questions map to multiple research questions as they address both perceived value (RQ2) and anticipated benefits for job performance and compliance (RQ3).

A.10 Summary: Question Distribution by DE Pillar

Table A.10: Question Distribution by Digital Engineering Pillar

DE Pillar	Questions
MBSE	Q2.1, Q3.4
Digital Twin	Q2.2, Q2.4, Q3.3
Digital Thread	Q2.3, Q2.5
PLM	Q2.6, Q3.5
General/All Pillars	Q1.1, Q1.2, Q3.1, Q3.2, Q3.6, Q4.1-Q4.5, Q5.1-Q5.7, Q6.1-Q6.4

A.11 Analysis Framework

A.11.1 Primary Analysis for Each Research Question

A.11.1.1 RQ1 Analysis (Awareness):

- Mean familiarity score (Q1.1) with 95% confidence interval
- Percentage with professional exposure (Q1.2) with 95% confidence interval
- Mean agreement scores for capability understanding (Q2.1-Q2.6)
- Percentage indicating agreement ($\geq$4) with each capability statement
- Comparison of awareness levels across professional fields (Q6.3) and experience levels (Q6.4)

A.11.1.2 RQ2 Analysis (Perceived Value):

- Mean agreement scores for applicability (Q3.1-Q3.2, Q3.6)
- Mean agreement scores for overall value (Q4.1, Q5.1)

- Percentage indicating investment willingness (Q4.5, Q5.7)
- Percentage indicating learning interest (Q6.1) and recommendation (Q6.2)
- Comparison of value perceptions across professional fields and experience levels

A.11.1.3 RQ3 Analysis (Job/Compliance Help):

- Mean agreement scores for specific benefits (Q4.2-Q4.4, Q5.2-Q5.6)
- Percentage agreeing with compliance benefits (Q3.5, Q3.6, Q5.6)
- Percentage agreeing with organizational capability benefits (Q3.3-Q3.5)
- Comparison of benefit perceptions across professional fields and experience levels

A.11.2 Composite Scores

Table A.11: Composite Score Definitions

Composite	Questions	Items	Interpretation
Awareness Composite	Q1.1, Q2.1-Q2.6	7	Higher = greater awareness/understanding
IT Value Composite	Q3.1, Q3.3-Q3.5, Q4.1-Q4.4	8	Higher = greater perceived IT value
Security Value Composite	Q3.2, Q3.6, Q5.1-Q5.6	8	Higher = greater perceived security value

Internal consistency shall be assessed via Cronbach's alpha (acceptable if $\alpha \geq 0.70$).

A.12 Scale Reference

A.12.1 Familiarity Scale (Q1.1)

Table A.12: Familiarity Scale

Score	Label	Interpretation
1	Not at all familiar	No awareness
2	Slightly familiar	Minimal awareness
3	Moderately familiar	Basic awareness
4	Very familiar	Good awareness
5	Extremely familiar	Expert awareness

A.12.2 Agreement Scale (Q2.1-Q5.6)

Table A.13: Agreement Scale

Score	Label	Interpretation
1	Strongly disagree	Strong negative perception
2	Disagree	Negative perception
3	Neither agree nor disagree	Neutral/uncertain
4	Agree	Positive perception
5	Strongly agree	Strong positive perception

A.12.3 Experience Level Categories (Q6.4)

Table A.14: Experience Level Categories

Category	Label	Career Stage
1-5 Years	Entry Level	Early Career
6-10 Years	Mid-Level (Early)	Mid Career
11-15 Years	Mid-Level (Late)	Mid Career
15+ Years	Senior Level	Late Career

Appendix B

Artificial Intelligence Assistance Disclosure

In accordance with academic integrity standards and emerging best practices for transparent research documentation, this appendix discloses the use of artificial intelligence tools in the preparation of this dissertation proposal. Such disclosure reflects the author's commitment to scholarly transparency and recognition of evolving norms within the academic community.

B.1 AI Tools Utilized

This dissertation proposal utilized Claude Opus 4.5, developed by Anthropic, to assist with specific aspects of document preparation. The AI tool was employed under the direct supervision of the author, with all outputs subjected to critical review, verification, and revision as necessary to ensure accuracy, appropriateness, and alignment with the research objectives. The author exercised editorial judgment over all AI-assisted contributions.

B.2 Scope of AI Assistance

AI assistance was limited to the following editorial and mechanical activities:

- Grammar and spelling review to identify and correct mechanical errors
- Sentence structure refinement to improve clarity and readability

- Organizational suggestions to enhance document flow and logical progression
- Formatting consistency verification across sections and chapters
- Citation format verification for compliance with IEEE standards

B.3 Scope Limitations

AI tools were explicitly excluded from the following substantive activities:

- Generation of original research ideas, hypotheses, or theoretical frameworks
- Literature search, source identification, or citation selection
- Data analysis, statistical calculations, or interpretation of results
- Writing of substantive original content without subsequent author revision
- Determination of research methodology or survey instrument design

The intellectual contributions of this research—the identification of research gaps, the development of the theoretical framework, the design of the survey instrument, and the interpretation of findings—remain solely the work of the author.

B.4 Author Responsibility

The author maintains full responsibility for all content, arguments, analyses, and conclusions presented in this dissertation. All AI-assisted text was critically reviewed and revised by the author to ensure it accurately represents the author's original thinking and research contributions. The employment of AI tools for editorial assistance does not diminish the author's intellectual ownership of this work, nor does it transfer scholarly credit for the ideas and arguments herein.

B.5 Rationale for Disclosure

This disclosure is provided in the spirit of transparency and in recognition of evolving academic standards regarding AI tool usage. As AI capabilities continue to advance, clear documentation of how these tools are employed in academic work supports research integrity and enables appropriate evaluation of scholarly contributions. The author believes that transparent disclosure serves the academic community better than silent utilization, and that establishing norms for responsible AI assistance in scholarly work represents an important contribution to academic discourse.