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

February 16, 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 Dissertation

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)
0.6	2026-JAN-31	Minor Updates: Include Ch. 1-3 & Appendices
0.7	2026-JAN-31	Added Timeline, Gantt Chart, and Schedule Milestones
0.8	2026-JAN-31	Rename main.tex to BonarDissertaation.tex, moved to github repo
0.9	2026-FEB-01	Minor Updates to correct grammar
0.10	2026-FEB-02	Updated Formatting of Appendix A & Minor Revisions
0.11	2026-FEB-03	Updated Acknowledgments
0.12	2026-FEB-07	Updates to Chapters 1-3 and Appendix A
0.13	2026-FEB-08	Updates to Chapters 1-3, Bibliography Updates
0.14	2026-FEB-08	Updates to Chapters 3, Bibliography Updates
0.15	2026-FEB-08	Updates to Chapters 1-2, Bibliography Updates
0.16	2026-FEB-08	Bibliography Updates
0.17	2026-FEB-15	Comprehensive rewrite of Chapters 1-2, additional citations
0.18	2026-FEB-15	Minor updates to address formatting and bibtex
0.19	2026-FEB-16	Added CMMC, Digital Twin Concerns, and sentence structure

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy in Cyber Operations degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

This page will be replaced by a signed page in the final version.

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 express my love and gratitude.

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, Doctor Kathryn 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 and friends whose wisdom has shaped my professional journey: Keith Summerson, Dale Kurth, Micah Mogle, Kavi Parupally, Nick Huggins, Doctor John Hastings, Doctor Kyle Cronin, Doctor Casey Mayfield, Kelly Ortberg, Greg Kouski, David Huston, Lyle Gillis, Josh Mason, Gene Drebenstedt, George, Karla Pepmeyer, and Charles Espy Jr. Though years may have passed since some of our paths crossed, your words of encouragement and guidance continue to resonate.

ABSTRACT

Digital Engineering has transformed how the Department of War, 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, where expanding compliance obligations—including the NIST Risk Management Framework, and the DoW Cybersecurity Maturity Model Certification—impose documentation, traceability, and verification demands that current practices fail to sustain. This research investigates whether IT and information assurance professionals recognize the potential that Digital Engineering capabilities hold for their work.

The research targets IT and information assurance professionals across multiple sectors, enabling assessment of whether Digital Engineering awareness and perceived value vary by organizational context. A quantitative survey collects 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 on professional awareness and perceived value, furnishing an evidence foundation for strategic decisions regarding future research investment, adoption initiatives, and curricula development. Results shall inform both scholarly inquiry and practical advancement of mission assurance capabilities.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another. I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

John James Darth Vader Bonar

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 cascading impact scope 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 model-based approaches are designed to accomplish with substantially greater efficiency [3].

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 [4]. 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. Cybersecurity, by contrast, refers specifically to the technical and operational dimensions of protecting systems from cyber threats. Both 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. Literature from defense and aerospace contexts suggests that Digital Engineering may address both dimensions: the governance and documentation requirements of information assurance and the operational visibility requirements of cybersecurity defense. Whether IT and information assurance professionals recognize this potential constitutes a central question of this research.

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) [4], the Information Technology Infrastructure Library (ITIL) [5], and the Unified Architecture Framework (UAF) [6].

1.1 Current State of Information System Management

Organizations today operate within an environment defined by relentless technological evolution and escalating system complexity. Cloud computing, microservices architectures, Internet of Things (IoT) devices, and operational technology have converged to spawn intricate webs of interdependencies that overwhelm traditional approaches to both information assurance and IT service delivery [7]. Such 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; con-

figuration management falters; security control implementation proceeds inconsistently across heterogeneous platforms [8].

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

Information assurance practice has evolved in response to the complexities of modern enterprise environments. Central to this evolution, the NIST Risk Management Framework provides a structured, disciplined approach for managing security and privacy risk that organizations can apply across diverse information systems [4]. RMF establishes a lifecycle approach to security through seven iterative steps: prepare, categorize, select, implement, assess, authorize, and monitor. Now foundational for federal agencies, the framework 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. Its 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 [9], the NIST Cybersecurity Framework [10], and COBIT [11], among others. 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 focuses upon the NIST Risk Management Framework, 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 [4]. Organizations operating outside federal requirements may employ alternative frameworks for control selection, including ISO/IEC 27001 [12], 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.

NIST Cybersecurity Framework (CSF) 2.0, released in February 2024, provides a voluntary, risk-based structure that complements the RMF by organizing cybersecurity outcomes into six core Functions: Govern, Identify, Protect, Detect, Respond, and Recover [13]. Version 2.0 added the Govern Function to address cybersecurity governance at the organizational level—a recognition that leadership engagement, risk strategy, and policy oversight constitute prerequisites for effective cybersecurity rather than ancillary concerns. Each Function decomposes into Categories and Subcategories that map to specific outcomes, and CSF 2.0 maintains explicit alignment with SP 800-53 controls through Informative References, enabling organizations to trace CSF outcomes to specific control implementations. Broadened in scope beyond critical infrastructure to encompass all organizations regardless of sector or size, CSF 2.0 serves as a bridging framework:

organizations subject to RMF compliance can use CSF to communicate risk posture to non-technical stakeholders, while organizations not subject to federal requirements can adopt CSF as a starting framework that maps naturally to SP 800-53 controls should compliance requirements evolve. CSF 2.0's emphasis upon governance, supply chain risk management, and continuous improvement aligns with Digital Engineering principles—particularly the authoritative source of truth concept and digital thread traceability—though no published research has examined this alignment.

Beyond federal systems, an expanding compliance landscape governs nonfederal organizations that process, store, or transmit Controlled Unclassified Information (CUI) on behalf of government agencies. NIST Special Publication 800-171 Revision 3, finalized in May 2024, establishes security requirements for protecting CUI in nonfederal systems and organizations [14]. Revision 3 restructured the framework from fourteen to seventeen security requirement families—adding Planning, System and Services Acquisition, and Supply Chain Risk Management—and aligned its control structure directly with SP 800-53 Revision 5 as the single authoritative source. SP 800-171's ninety-seven requirements encompass 266 individual control items and forty-nine Organization-Defined Parameters that provide implementation flexibility while enabling automated compliance assessment through machine-readable formats such as the Open Security Controls Assessment Language (OSCAL) [15]. CSF 2.0 maps to SP 800-171 requirements through shared SP 800-53 lineage: organizations implementing SP 800-171 controls simultaneously address CSF Subcategory outcomes in the Identify, Protect, Detect, Respond, and Recover Functions, creating a unified compliance posture across both frameworks.

NIST Special Publication 800-172 supplements the SP 800-171 baseline with thirty-five enhanced security requirements designed to protect CUI associated with critical programs and high-value assets against Advanced Persistent Threats [16]. Operating upon a three-pillar defense strategy—penetration-resistant architecture, damage-limiting operations, and cyber resiliency and survivability—SP 800-172 demands capabilities that

manual processes and static documentation struggle to sustain. Enhanced requirements span access control, configuration management, identification and authentication, incident response, risk assessment, situational awareness, and system protection. A Revision 3 update currently in development expands scope from confidentiality protection alone to encompass confidentiality, integrity, and availability, further increasing documentation and verification demands.

Operationalizing these NIST requirements within the defense industrial base, the Cybersecurity Maturity Model Certification (CMMC) 2.0 framework establishes a three-tiered certification structure [17]. Level 1 requires fifteen foundational practices for Federal Contract Information protection through annual self-assessment. Level 2 mandates compliance with the 110 requirements of SP 800-171 Revision 2, assessed through triennial third-party evaluation by CMMC Third-Party Assessment Organizations. Level 3 adds twenty-four enhanced requirements drawn from SP 800-172, assessed by the Defense Industrial Base Cybersecurity Assessment Center. Phase 1 implementation commenced with the December 2024 effective date of 32 CFR Part 170, with full implementation across all contracts involving Federal Contract Information or Controlled Unclassified Information expected by November 2028. CMMC represents a fundamental shift from self-attestation to verified compliance, imposing documentation and evidence requirements that intensify the challenges organizations already face in maintaining accurate, current security documentation. Across this expanding compliance landscape—from CSF 2.0's voluntary governance framework through SP 800-171 and SP 800-172's CUI protection requirements to CMMC's third-party verification mandate—organizations confront escalating documentation, traceability, and verification demands that Digital Engineering capabilities are designed to address.

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, ser-

vice operation, and continual service improvement [5]. 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. Rather, it 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 [18]. Studies find that organizations can monitor only sixty-six percent of their IT environments, leaving thirty-four percent unmonitored [19]. 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 [20]. The mean time to identify security breaches averages 204 days, reflecting the visibility gaps that impair threat detection [21].

These statistics represent not merely organizational shortcomings but systemic limi-

tations 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. Modern IT environments change at rates exceeding 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 [22]. Originally forged within the defense and aerospace sectors, Digital Engineering has been formalized through authoritative guidance from organizations including the United States Department of War (DoW) [23], the National Aeronautics and Space Administration

(NASA) [24], and the International Council on Systems Engineering (INCOSE) [22]. 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.

Digital Engineering's emergence from defense and aerospace contexts carries significance beyond historical interest. Both sectors developed these 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. Solutions that proved effective for managing combat aircraft development and spacecraft missions may prove equally effective for managing enterprise information systems and security postures. Measured evidence supports this potential: Rogers and Mitchell documented an eighteen percent improvement in systems engineering efficiency and a nine percent reduction in defects following MBSE adoption on a complex system-of-systems program [25]. Yet such measured evidence remains rare, and no comparable data exist for enterprise IT or Information Assurance contexts.

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 [26]. 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 [27].

The distinction between document-centric and model-centric approaches warrants emphasis because it defines the fundamental transformation that Digital Engineering proposes. 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. When an organization produces a network diagram, that diagram captures system state at the moment of creation. Every subsequent change renders the diagram incrementally less accurate. When an organization writes a security plan, that plan describes intended security posture at the time of writing. Every subsequent system modification creates potential divergence between the plan and operational reality. 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. This automated consistency maintenance addresses the fundamental velocity mismatch between documentation processes and operational change rates that undermines current information assurance and IT service management practices.

Formal modeling languages underpin MBSE implementations and provide the techni-

cal foundation for these capabilities. SysML, the Systems Modeling Language standardized through the Object Management Group, extends the Unified Modeling Language (UML) with constructs specifically designed for systems engineering [28]. Where UML focuses upon software system modeling, SysML adds requirements modeling, parametric analysis, and physical system representation that UML lacks. SysML defines nine diagram types organized into four pillars: requirements diagrams for capturing and tracing stakeholder requirements; structure diagrams including block definition diagrams and internal block diagrams for representing system architecture, composition, and interconnections; behavior diagrams including activity diagrams, sequence diagrams, and state machine diagrams for modeling system dynamics and operational processes; and parametric diagrams for expressing constraint relationships and enabling quantitative analysis. This diagram taxonomy provides a comprehensive vocabulary for representing complex systems from multiple perspectives simultaneously—a capability that directly supports the multi-stakeholder visibility requirements of both information assurance governance and IT service management coordination.

The evolution from SysML 1.x to the emerging SysML v2 specification addresses limitations that impeded broader adoption. SysML v2 introduces a redesigned language architecture emphasizing improved precision, expressiveness, and usability. The new specification provides a standardized textual notation alongside the graphical notation, enabling model creation through text-based interfaces more familiar to software developers and IT professionals. SysML v2 also introduces a standardized Application Programming Interface (API) for tool interoperability, addressing a persistent criticism that MBSE tool ecosystems require vendor-specific integrations. This improved interoperability reduces the vendor lock-in concerns that organizations evaluating MBSE adoption frequently cite. For enterprise IT contexts, the textual notation and API standardization lower adoption barriers by aligning MBSE practices more closely with the text-based configuration and automation workflows that IT professionals employ daily.

The MBSE tool ecosystem encompasses both commercial and open source platforms. Commercial tools—including Dassault SystÃfÂ¨mes Cameo Systems Modeler and IBM Engineering Systems Design Rhapsody—provide comprehensive modeling environments with enterprise support, training resources, and integration capabilities developed through decades of aerospace and defense application. Open source alternatives have emerged primarily through the Eclipse Foundation's modeling ecosystem. Eclipse Papyrus provides an open source UML and SysML modeling environment [29]. Capella, developed by Thales and contributed to Eclipse, provides a comprehensive MBSE tool implementing the Arcadia methodology, achieving significant industrial adoption across aerospace, energy, and transportation sectors [30]. SysON, currently under development, implements the SysML v2 specification with a modern web-based architecture designed for collaborative modeling [31]. These open source tools reduce economic barriers to MBSE adoption. However, their documentation, community resources, and application examples focus predominantly upon traditional systems engineering domains. Organizations seeking to apply MBSE tools for enterprise IT or Information Assurance purposes must adapt without domain-specific guidance—an adaptation that remains unexplored in the academic literature.

Architecture frameworks provide the structural foundation for organizing MBSE implementations. Within MBSE practice, architecture frameworks define the viewpoints, views, and model elements that architects employ to represent systems. UAF, discussed in detail in a subsequent subsection, provides the most comprehensive architecture framework for MBSE implementations spanning both defense and commercial domains. Its 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, enabling representation of security controls, operational processes, service dependencies, and resource allocations within a single integrated model environment.

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. However, achieving this integration requires modeling language extensions and domain-specific profiles that have not yet been developed or validated for enterprise IT contexts. SysML provides excellent support for modeling physical systems with requirements, behaviors, and structures, but modeling IT services, network configurations, and security controls requires adaptation or extension that practitioners must develop independently. The absence of standardized approaches for modeling enterprise IT in SysML constitutes a technical barrier to adoption that accompanies the awareness and perception barriers this research investigates.

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 [32]. The term 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 [33].

The concept of authoritative traceability deserves careful attention because it addresses a fundamental limitation of current information assurance and IT service management practice. 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. A requirements traceability matrix that maps security controls to implementation artifacts represents a snapshot of intended relationships at the time of creation. Every subsequent change to either controls or implementations creates potential inconsistency that manual processes may not detect. 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. This automated currency maintenance distinguishes digital threads from the manual traceability approaches that current compliance practices employ.

The Department of Defense Digital Engineering Strategy positions the digital thread as essential infrastructure for achieving the authoritative source of truth—the single, trusted baseline of system information from which all stakeholders operate [3]. As a concept, the authoritative source of truth addresses a persistent challenge in both defense acquisition and enterprise IT management: when multiple documentation artifacts describe the same system, discrepancies inevitably emerge, and no definitive mechanism exists for determining which artifact accurately reflects operational reality. Digital threads resolve this challenge by establishing verified connections between all system artifacts, ensuring

that changes propagate consistently and that queries return authoritative rather than potentially obsolete information. The Systems Engineering Research Center has produced foundational research supporting digital thread implementation, including the Enterprise System-of-Systems Model for Digital Thread Enabled Acquisition, which establishes architectural patterns for maintaining traceability across complex, multi-system environments [34]. DoDI 5000.97 codifies these concepts into mandatory requirements, directing defense programs to maintain digital thread capabilities throughout the acquisition lifecycle [35].

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. When a security control implementation changes, digital thread connections enable automated identification of affected requirements, dependent controls, and compliance documentation requiring update. When auditors require evidence of control implementation, digital threads provide navigable paths from requirements through implementation to assessment results without requiring manual evidence compilation.

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. When a proposed change affects a configuration item, digital

thread connections reveal which services depend upon that item, which security controls protect it, and which compliance requirements govern it. 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.

The practical implementation of digital threads requires integration infrastructure that connects diverse tools and repositories. In defense contexts, this integration has developed over years of investment and standardization. Enterprise IT environments employ different tool ecosystems—IT service management platforms like ServiceNow and BMC, security information and event management systems, cloud management consoles, and configuration automation tools—that were not designed with digital thread connectivity in mind. Establishing digital thread capabilities in enterprise IT contexts therefore requires integration approaches that bridge systems engineering tools and IT management platforms. This integration challenge represents a practical barrier that accompanies the conceptual transfer of digital thread principles from defense to enterprise IT contexts.

1.2.3 Digital Twin Technology

Digital twin technology creates virtual replicas of physical or logical systems that maintain synchronization with their real-world counterparts through continuous data exchange [36]. These virtual representations enable organizations to simulate system behavior, analyze potential changes, predict future states, and optimize performance without disrupting operational systems [37]. Digital twins combine real-time operational data with analytical models to provide dynamic, predictive capabilities that extend far beyond traditional monitoring and simulation approaches [38].

As a concept, the digital twin originated in Product Lifecycle Management research. Grieves traces the evolution of digital twins from their conceptual origins through contemporary applications, positioning digital twins as the integration of physical and virtual

spaces that enables analysis, optimization, and prediction across system lifecycles [39]. A foundational distinction between digital twins and traditional simulation lies in synchronization: where traditional simulations model hypothetical or designed system states, digital twins maintain continuous data exchange with their physical or logical counterparts, enabling operational decision-making based upon current rather than documented system states. Synchronization directly addresses the documentation-reality gap that undermines information assurance and IT service management practices. Static models represent intended or designed system states; digital twins represent current operational states, updated continuously through integration with operational data sources. This distinction carries profound implications for organizations that must make security and operational decisions based upon accurate understanding of system configurations.

Standardization efforts have established frameworks for digital twin implementation that reduce interoperability concerns and provide structured guidance. The International Organization for Standardization published ISO 23247, the Digital Twin Framework for Manufacturing, defining a four-part reference architecture encompassing observable manufacturing elements, digital twin entities, data collection and device control infrastructure, and cross-domain integration [40]. Shao et al. provided detailed analysis of ISO 23247's structure and applicability [41]. While developed for manufacturing contexts, the reference architecture establishes patterns—data synchronization, entity representation, cross-domain integration—that inform digital twin implementations in other domains. IEC 62832 complements ISO 23247 by addressing industrial-process measurement, control, and automation aspects of digital twin frameworks [36]. In parallel, the Internet Engineering Task Force has published a draft reference architecture specifically addressing network infrastructure digital twins, representing direct engagement with the IT infrastructure domain [42]. IETF engagement signals that the networking community has recognized digital twin applicability for IT infrastructure, though the published architecture remains at draft stage and has not yet achieved the maturity of manufacturing-focused

standards.

NIST has engaged with digital twin technology through NIST Internal Report 8356, which addresses cybersecurity challenges and trust considerations for digital twin implementations [43]. Notably, this publication examines security considerations *for* systems employing digital twins rather than digital twin applications *to* Information Assurance—a distinction that reveals the current orientation of institutional research. NIST's Framework for Cyber-Physical Systems similarly addresses digital integration challenges at the intersection of physical and computational systems [44]. Together, these publications establish that authoritative institutions recognize digital twin relevance to security domains while treating digital twins primarily as systems requiring security rather than as tools for enhancing security operations. The reorientation from securing digital twins to employing digital twins for security purposes represents a conceptual shift that the academic literature has begun but not yet completed.

Open source frameworks have emerged to reduce economic and technical barriers to digital twin adoption. The Digital Twin Consortium has established an open source collaboration initiative providing frameworks and reference implementations [45]. Eclipse Ditto, maintained by the Eclipse Foundation, provides an open source framework for creating and managing digital twins in Internet of Things applications [46]. Eclipse BaSyx implements the Asset Administration Shell standard for industrial digital twins [47]. Gil et al. conducted a systematic survey of fourteen open source digital twin frameworks, evaluating them against criteria derived from ISO 23247 standards and finding significant variation in maturity, documentation quality, and community support [48]. Autiosalo et al. introduced Twinbase, an open source server for the Digital Twin Web concept, enabling organizations to publish and discover digital twin descriptions through standardized interfaces [49]. These open source options provide accessible entry points for organizations exploring digital twin capabilities, though their documentation and application examples focus upon manufacturing and IoT rather than enterprise IT or Information Assurance

contexts.

In information assurance contexts, digital twin capabilities offer advantages for security control validation, risk assessment, and incident response. 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. The ability to simulate adversary behavior against synchronized representations of actual system configurations enables security testing that reflects operational reality rather than documented assumptions.

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. When combined with digital thread traceability, digital twins enable organizations to assess the security and operational implications of proposed changes simultaneously—an integrated analysis capability that current practices, which typically assess security and operational impacts through separate processes, cannot provide.

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 [50]. 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.

PLM originated in manufacturing and product development, where organizations confronted the challenge of managing complex products involving thousands of components, multiple suppliers, extended development timelines, and rigorous quality requirements. Manufacturing organizations developed PLM practices to address challenges that bear structural similarity to those confronting enterprise IT management: maintaining accurate documentation of complex configurations, coordinating changes across interdependent components, ensuring consistency between design documentation and as-built products, and managing compliance with regulatory requirements throughout product lifecycles. Over decades of industrial application, the commercial PLM ecosystem has matured, producing platforms that manage millions of engineering artifacts across global supply chains. Open source PLM alternatives have emerged to reduce cost barriers, though Campos et al. noted that industrial open source PLM solutions vary considerably in maturity and require careful evaluation against organizational requirements [51].

The application of PLM principles to information systems represents a conceptual extension from these manufacturing origins. 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, where system components are logical rather than physical, change cycles occur in hours rather than months, and deployment involves software configurations

rather than manufacturing processes.

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 configuration baseline capabilities directly address the requirement in NIST SP 800-53 control CM-2 for documented, maintained system baselines [4]. PLM change coordination capabilities support control CM-3 requirements for configuration change control. PLM access governance capabilities align with CM-5 requirements for access restrictions governing system changes. These correspondences between PLM capabilities and specific compliance requirements suggest that PLM practices could address compliance obligations that organizations currently struggle to fulfill through manual processes.

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. PLM's emphasis upon managing information across organizational boundaries addresses the silo problem that fragments visibility in current IT environments: security teams, operations teams, and application teams can operate from a shared, au-

thoritative information base rather than maintaining separate, potentially inconsistent documentation.

1.2.5 Institutional Endorsement and Strategic Direction

Digital Engineering's maturation from experimental practice to institutional mandate provides important context for evaluating its potential applicability beyond defense and aerospace. The breadth and depth of institutional endorsement establishes that Digital Engineering represents not an experimental approach advocated by enthusiasts but a mature discipline validated by the organizations most experienced in managing complex, compliance-intensive systems. Understanding this institutional foundation informs assessment of whether Digital Engineering merits investigation for enterprise IT and Information Assurance applications.

Published in June 2018, the Department of Defense Digital Engineering Strategy established the formal vision for transforming defense acquisition through Digital Engineering practices [3]. Five strategic goals collectively articulate the transformation Digital Engineering envisions: formalize the development, integration, and use of models to inform enterprise and program decision-making; provide an authoritative source of truth by establishing a digital thread as the means of delivering the technical baseline; incorporate technological innovation to improve the engineering practice; establish a Digital Engineering ecosystem to provide the infrastructure and environments for performing Digital Engineering activities; and transform the culture and workforce to adopt and support Digital Engineering across the lifecycle. Notably, these goals extend beyond technology adoption to encompass organizational transformation, workforce development, and cultural change—dimensions that any transfer of Digital Engineering to enterprise IT contexts must address.

DoD Instruction 5000.97, issued in December 2023, codified these strategic aspirations into mandatory requirements for defense programs [35]. It mandates that programs

leverage digital artifacts as the authoritative source of system information and maintain digital thread capabilities throughout the acquisition lifecycle. Moving from strategic vision to regulatory mandate represents a significant institutional commitment: defense programs must now implement Digital Engineering practices rather than merely consider them. Complementing this mandate, the Systems Engineering Guidebook provides detailed implementation guidance for meeting these requirements, establishing processes, methods, and tool expectations for Digital Engineering practice within defense acquisition [23]. A clear progression from strategy document to formal instruction to implementation guidebook demonstrates institutional maturation that parallels the compliance framework progression familiar in information assurance contexts—from policy through standards through implementation guidance.

NASA has pursued a parallel path toward Digital Engineering adoption, lending independent validation to the approach. NASA-HDBK-1004, the NASA Digital Engineering Acquisition Framework Handbook, establishes guidance for incorporating Digital Engineering practices into NASA programs [52]. A companion document, the NASA Future Model-Based Systems Engineering Vision and Strategy Bridge, articulates NASA's long-term vision for MBSE adoption across the agency's portfolio of complex, mission-critical programs [53]. NASA's independent development of Digital Engineering guidance carries particular significance: both the Department of War and NASA confronted similar challenges—complex systems demanding comprehensive documentation, stringent compliance requirements, mission-critical operations tolerating no ambiguity in system understanding—and both converged upon Digital Engineering as the solution. This independent convergence strengthens the argument that Digital Engineering addresses fundamental challenges in managing complex, compliance-intensive systems rather than representing a domain-specific solution applicable only to defense acquisition.

INCOSE has positioned Digital Engineering as the future direction of the systems engineering discipline. Its Systems Engineering Vision 2035 establishes a roadmap for trans-

forming systems engineering practice through Digital Engineering, model-based methods, and integrated digital environments [54]. Complementing this vision, the INCOSE Systems Engineering Handbook, Fifth Edition, provides comprehensive guidance for implementing systems engineering practices including MBSE, reflecting the discipline's current state of practice and serving as the primary professional reference for systems engineers worldwide [55]. INCOSE's Digital Engineering Information Exchange Working Group specifically addresses the interoperability and integration challenges that arise when organizations attempt to exchange digital engineering artifacts across organizational and tool boundaries [22]. This working group's existence acknowledges that Digital Engineering implementation requires addressing practical interoperability challenges—challenges that would intensify when extending Digital Engineering beyond its established systems engineering context into enterprise IT domains.

The Systems Engineering Body of Knowledge (SEBoK), jointly managed by INCOSE, the IEEE Systems Council, and the Stevens Institute Systems Engineering Research Center, provides the globally recognized authoritative reference defining Digital Engineering's relationship to MBSE, digital threads, and authoritative sources of truth within the ISO/IEC/IEEE 15288:2023 systems engineering lifecycle framework [56]. SEBoK establishes the conceptual vocabulary and architectural relationships that the systems engineering community employs when discussing Digital Engineering, providing the definitional foundation upon which this dissertation's investigation builds.

SERC has produced foundational research publications supporting Digital Engineering implementation and assessment. Its Digital Engineering Competency Framework defines 962 Knowledge, Skills, Abilities, and Behaviors organized by proficiency levels, providing the most comprehensive specification of what professionals require to practice Digital Engineering effectively [27]. A companion Digital Engineering Metrics framework establishes measurement approaches for assessing adoption progress and benefits realization, addressing the measurement challenge that the literature identifies as a persistent barrier

to evidence-based adoption decisions [26]. Additionally, the SERC Systems Engineering Modernization report examines the integration of Digital Engineering with Mission Engineering, Agile, and DevOps practices, establishing connections between Digital Engineering and the development methodologies prevalent in enterprise IT contexts [57]. Collectively, these SERC publications provide the research infrastructure—competency definitions, metrics, and integration frameworks—that would support Digital Engineering adoption in new domains, including enterprise IT and Information Assurance.

NIST's contributions span multiple relevant domains. The Framework for Cyber-Physical Systems addresses integration challenges at the intersection of physical and computational systems [44]. NIST's systems security engineering publications—Special Publication 800-160 Volume 1 Revision 1 on Engineering Trustworthy Secure Systems [50] and Volume 2 Revision 1 on Developing Cyber-Resilient Systems [58]—reference model-based approaches and traceability requirements that align with Digital Engineering principles. NIST Internal Report 8356 on digital twin security considerations [43] and the Open Security Controls Assessment Language initiative [15] further demonstrate NIST engagement with concepts that Digital Engineering could integrate. Taken together, these publications establish that the institution responsible for federal cybersecurity standards recognizes the relevance of model-based approaches, traceability, and digital integration to security engineering—even though NIST has not yet explicitly connected these concepts under the Digital Engineering framework or provided specific guidance for their application in enterprise IT contexts. A pronounced gap between NIST's recognition of relevant principles and the absence of specific Digital Engineering implementation guidance for enterprise IT constitutes one of the research gaps this dissertation addresses.

1.2.6 Enterprise Architecture Frameworks

Enterprise architecture frameworks provide the structural foundation upon which Digital Engineering implementations rest. These frameworks define how organizations represent,

analyze, and manage the complex relationships among business processes, information flows, application systems, and technology infrastructure. Understanding the enterprise architecture framework ecosystem is essential for evaluating Digital Engineering's potential in enterprise IT contexts because the frameworks determine what can be modeled, how models are organized, and what analytical capabilities models support.

The Unified Architecture Framework, now codified as ISO/IEC 19540 through the Object Management Group [6], represents the most significant evolution in enterprise architecture standardization. UAF emerged from the consolidation of military architecture frameworks—the Department of Defense Architecture Framework (DoDAF) [59], the UK Ministry of Defence Architecture Framework (MODAF), and the NATO Architecture Framework [60]—with the explicit recognition that the architectural concepts developed for military system-of-systems management possess broad applicability beyond defense contexts. The Object Management Group determined that approximately ninety percent of concepts captured in military architecture frameworks prove equally applicable in commercial domains [61], motivating the development of a unified framework that serves both defense and commercial organizations without requiring domain-specific adaptations.

UAF employs a grid-based structure defining seventy-one view specifications organized through two complementary specifications: the UAF Domain Metamodel (DMM), which defines the underlying concepts, relationships, and constraints; and the UAF Modeling Language (ML), which provides the concrete notation for expressing architecture descriptions [62]. Grid rows represent stakeholder domains—Strategic, Operational, Services, Personnel, and Resources—while columns represent architecture aspects including taxonomy, structure, connectivity, processes, states, interaction, constraints, and traceability. Together, this grid organization enables architects to represent any complex system-of-systems from multiple stakeholder perspectives simultaneously, with formal relationships connecting views across the grid to maintain consistency. Notably, the traceability column explicitly addresses the requirement for maintaining verified connections across architec-

tural perspectives—a requirement that aligns directly with the digital thread concept and with the compliance traceability obligations that NIST SP 800-53 imposes.

The evolution from domain-specific frameworks to the unified standard proceeded through several stages. DoDAF 2.0 established the foundational metamodel for defense architecture description [59]. MODAF independently developed architecture description conventions for UK defence applications. The NATO Architecture Framework provided architecture capabilities for alliance-wide interoperability [60]. Earlier evaluation identified limitations in these individual frameworks: the National Defense Industrial Association Systems Engineering Division found that DoDAF required augmentation to adequately support systems engineering activities [63], and research by Hause identified specific gaps between DoDAF's metamodel and the requirements of model-based systems engineering practice [64]. The Unified Profile for DoDAF and MODAF (UPDM) represented an initial consolidation effort that eventually evolved into UAF under broader OMG stewardship, with ISO/IEC international standardization following to establish UAF as a globally recognized rather than organizationally specific standard [65].

Comparative research validates UAF's position relative to alternative enterprise architecture frameworks. Bankauskaite evaluated enterprise architecture frameworks using weighted criteria encompassing completeness, maturity, standardization, and tool support, finding that UAF achieved the highest overall rating among the frameworks evaluated, surpassing TOGAF [67], DoDAF, MODAF, NAF, and FEAF [66]. This comparative advantage derives from UAF's comprehensive metamodel, its ISO international standardization, and its explicit design for both defense and commercial applications. Research by Eichmann et al. demonstrated UAF application to system-of-systems development [68]. Liu et al. applied UAF to military system-of-systems design using top-down MBSE methodology [69]. Torkjazi et al. extended UAF-based MBSE to integrate autonomy into system-of-systems architectures [70]. Abhaya established UAF-Based MBSE methods for building system-of-systems models [71]. Collectively, these studies demon-

strate UAF's growing adoption and validation across diverse system-of-systems contexts, though applications to enterprise IT infrastructure and Information Assurance remain absent from the published literature.

The complementary relationship between UAF and the commercially prevalent Open Group Architecture Framework (TOGAF) reduces adoption barriers for organizations already invested in enterprise architecture practice. TOGAF provides a comprehensive architecture development method and enterprise architecture governance framework widely adopted in commercial IT contexts [67]. A joint white paper between The Open Group and MITRE Corporation established that UAF and TOGAF address different but complementary aspects of enterprise architecture: TOGAF provides the methodology and governance framework for architecture development, while UAF provides the architecture description specification for expressing what has been architected [72]. Organizations can retain TOGAF methodology while adopting UAF for architecture description, enabling incremental adoption rather than wholesale replacement of established practices. This compatibility carries particular significance for enterprise IT organizations that have invested in TOGAF-based architecture programs, as it suggests that UAF adoption for model-based architecture description need not require abandonment of existing architecture governance investments.

UAF's foundation upon UML and SysML profiles enables model-based documentation approaches that address the accuracy and currency challenges plaguing traditional enterprise architecture implementations [73]. Because UAF architecture descriptions are expressed as formal models rather than static documents, they inherit the automated consistency checking, impact analysis, and traceability capabilities that model-based approaches provide. A model-based foundation connects enterprise architecture practice to the broader Digital Engineering ecosystem: UAF models can participate in digital threads, maintain synchronization with operational systems through digital twin mechanisms, and be managed through PLM lifecycle processes. Adoption of UAF by the Department of

War [23], NATO [60], and the UK Ministry of Defence, combined with ISO international standardization, establishes UAF as the authoritative consolidating framework for organizations requiring architecture capabilities across multiple domains. For enterprise IT and Information Assurance applications, UAF provides structured approaches to documenting systems, relationships, and security requirements that align with both NIST and ITIL expectations. Understanding this enterprise architecture foundation provides essential context for evaluating how Digital Engineering extends architectural approaches from static documentation toward living, model-based representations that maintain currency with operational reality.

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. Digital Engineering practices have demonstrated capabilities in defense and aerospace contexts that address structurally analogous challenges: maintaining authoritative documentation, ensuring configuration visibility, and providing traceability across complex systems [3]. Whether these capabilities translate to enterprise IT and information assurance contexts, and whether professionals in those domains recognize the potential relevance, remains uninvestigated. Examining the specific gaps that persist in current practice illuminates the structural parallels that motivate this investigation.

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. Visibility gaps manifest throughout the RMF lifecycle: organizations find it difficult to track security dependencies effectively, leading to unidentified vulnerabilities when changes are implemented. 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. Such assessment requires understanding of system dependencies that current documentation approaches cannot maintain. 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 con-

trols from NIST SP 800-53 across diverse platforms while supporting continuous deployment practices and rapid update cycles [4]. 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 [18]. 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 a candidate alternative approach whose demonstrated benefits in defense and aerospace contexts suggest potential applicability to enterprise IT environments.

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 in-

frastructure. 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 offers capabilities designed to address 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. Defense and aerospace organizations have demonstrated these capabilities in complex, compliance-intensive environments [3]. The question this research investigates is whether IT and information assurance professionals recognize the potential value of these capabilities for their work—a prerequisite question for determining whether Digital Engineering practices developed in defense contexts merit investigation for broader enterprise application.

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. Preliminary evidence from adjacent domains suggests that such investigation is urgently needed: Henderson et al. found that approximately twenty-two percent of systems engineering professionals—practitioners within the discipline that developed MBSE—could not articulate a clear definition of MBSE [74]. If awareness deficits persist within the originating discipline, awareness among professionals in Information Assurance and IT Service Management—disciplines that have never

systematically encountered these methodologies—requires empirical measurement rather than assumption.

The distinction between Research Question 2 and Research Question 3 warrants explicit clarification, as both address professional perceptions of Digital Engineering value. Research Question 2 measures whether professionals recognize Digital Engineering capabilities as abstractly valuable or important for their professional domains—an assessment of general relevance that does not require the respondent to evaluate specific operational impact within their own work context. Research Question 3 probes a more personal and practical construct: whether professionals believe Digital Engineering could tangibly help them perform their jobs, meet the compliance requirements they personally face, or enhance the specific organizational capabilities they are responsible for delivering. Technology adoption literature distinguishes between recognizing that a capability has general value and believing that the same capability would improve one's own work. Professionals may acknowledge that Digital Engineering offers theoretical value for their domain while remaining skeptical about its practical applicability to their specific organizational context. This distinction carries significant implications for adoption strategy: a professional community that perceives general value but doubts personal applicability requires different intervention than one that perceives both.

1.5 Research Scope and Approach

Across several key areas, this research examines professional perceptions. 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 percep-

tions 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.

1.5.2 Target Population

The research targets IT and information assurance professionals across diverse organizational contexts. Included in this population are security analysts, compliance officers, IT managers, network administrators, systems administrators, and other professionals who implement and maintain information assurance controls or deliver IT services. By surveying professionals across organizational contexts rather than limiting investigation to a single industry or organization, the research enables assessment of awareness and perceived value across the professional community.

The target population intentionally extends beyond the systems engineering professionals who have been the focus of previous MBSE adoption research. While studies by Call et al. and Henderson et al. examined perceptions among systems engineering professionals [74], [75], no comparable research addresses IT and Information Assurance practitioners. This population represents a crucial test of Digital Engineering's transferability:

if professionals who have never encountered these methodologies nevertheless recognize their potential value for addressing familiar challenges, the case for cross-disciplinary investigation strengthens substantially.

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. Automated traceability provided by digital threads could reduce the manual effort required for compliance audits. Model-based documentation enabled by MBSE could maintain accuracy through automated synchronization rather than manual updates. Configuration management capabilities offered by PLM 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. Rather, 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 recog-

nize 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. 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. Such 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.

Building 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 [76], 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

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

Empirical evidence is contributed by this research to a domain currently characterized by theoretical proposition rather than data. Perception data collected from working professionals enables assessment of whether the theoretical framework connecting Digital Engineering capabilities to documented IT and information assurance challenges resonates with practitioners who experience those challenges directly. Findings indicating that professionals recognize value in Digital Engineering capabilities would validate the theoretical premise and support subsequent implementation research. Findings indicating limited awareness or skepticism would redirect the research agenda toward education initiatives or reconsideration of transferability assumptions. Either outcome advances the academic understanding of Digital Engineering's potential applicability beyond its established defense and aerospace foundations.

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.

Beyond individual organizations, the research identifies which specific Digital Engineering capabilities professionals perceive as most valuable for their work. Such 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 dissertation: maintaining accurate documentation, implementing consistent security controls, and verifying compliance across complex technical environments.

Digital threads, as demonstrated in defense applications, enhance compliance verification and security assurance by providing authoritative traceability—verified connections between security requirements, control implementations, and compliance evidence [3]. Operators of federal and national security 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 offer the potential to 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 are designed to provide the visibility and traceability that enable rapid, accurate impact assessment—capabilities that current approaches demonstrably fail to provide. Whether these capabilities can be realized effectively outside defense and aerospace contexts remains an open question that this research begins to address through professional perception data.

1.6.4 Societal Significance

Beyond organizations operating national security systems, Digital Engineering capabilities may 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.

If Digital Engineering practices prove transferable beyond defense and aerospace contexts, their documentation and traceability capabilities could reduce the time and specialized knowledge required for compliance verification, potentially 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 may 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 extend sophisticated security and documentation capabilities to resource-constrained organizations represents a motivating consideration for this research. Currently, enterprise architecture, authoritative traceability, and model-based documentation remain accessible primarily to large organizations with specialized expertise and dedicated budgets. This research does not directly investigate adoption within resource-constrained organizations. However, by establishing whether IT and information assurance professionals broadly perceive value in Digital Engineering capabilities, the findings create a foundation for subsequent research examining practical applicability across diverse organizational contexts, including those serving underrepresented populations.

1.7 Chapter Summary

In establishing the context for investigating professional awareness and perceptions of Digital Engineering capabilities within information assurance and IT service management domains, this chapter has 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 that have demonstrated value in defense and aerospace contexts and that may address analogous gaps in enterprise IT and information assurance practice. The institutional endorsement of Digital Engineering

by the Department of War, NASA, INCOSE, and standards bodies including the Object Management Group and ISO establishes the maturity and authoritative standing of these methodologies, while enterprise architecture frameworks—particularly the Unified Architecture Framework—provide the structural foundation for implementation.

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. Significance 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 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 through a sustained analytical synthesis that identifies not merely what the literature contains but what debates remain unresolved, what tensions persist between proven capability and limited adoption, and why the present

research is necessary.

Chapter 2

Literature Review

The literature on Digital Engineering tells a story of proven capability confined within disciplinary walls. Model-Based Systems Engineering, digital threads, digital twins, and Product Lifecycle Management have matured through decades of application in defense and aerospace, accumulating institutional endorsement from the Department of War, NASA, and INCOSE alongside rare but compelling empirical evidence of return on investment. Yet this maturation has occurred almost entirely within the systems engineering discipline. Enterprise IT infrastructure management and Information Assurance—domains that confront structurally analogous challenges of documentation accuracy, configuration visibility, compliance traceability, and change coordination—have developed independently, producing their own frameworks, their own tools, and their own patterns of persistent failure. The result is a pronounced research gap: apart from a preliminary reference model by Bonar and Hastings [76] and a conceptual framework for DevSecOps security assurance from the Carnegie Mellon Software Engineering Institute [77], no peer-reviewed research addresses the application of Digital Engineering methodologies to enterprise IT infrastructure, IT Service Management, or Information Assurance programs broadly.

Why that gap persists and why it matters forms the central inquiry of this chapter. Proceeding through an analytical synthesis of research spanning MBSE value evidence, adoption dynamics, cross-disciplinary transfer barriers, digital twin security applications,

compliance automation, IT service management failures, and enterprise visibility challenges. Rather than cataloging what exists, the review foregrounds the debates, tensions, and unresolved questions that position this dissertation's investigation within the academic conversation. Three interrelated arguments emerge. First, the evidence base for MBSE value, while growing, remains disproportionately reliant upon perceived rather than measured outcomes, creating economic uncertainty that discourages adoption beyond established domains. Second, adoption research demonstrates that perceptions—not objective technical merit—drive adoption decisions, yet no empirical data exist on how IT and Information Assurance professionals perceive Digital Engineering capabilities. Third, compliance frameworks and IT service management standards explicitly require capabilities that Digital Engineering provides, yet the academic community has not investigated whether Digital Engineering could fulfill these requirements more effectively than traditional approaches that demonstrably fail.

2.1 The Evidence Paradox: Demonstrated Value Without Sufficient Proof

The case for Model-Based Systems Engineering rests upon a paradox that shapes the entire adoption landscape: practitioners and organizations widely perceive MBSE as valuable, yet rigorous empirical measurement of that value remains exceptionally rare. Understanding this paradox is essential because it explains both why MBSE has succeeded within systems engineering and why it has not expanded beyond it. Organizations already embedded in the systems engineering discipline can rely upon institutional experience and professional networks to validate MBSE investment. Organizations outside the discipline—including enterprise IT and Information Assurance—lack comparable experiential evidence and must rely upon published research that, as the literature reveals, provides insufficient quantitative justification.

Among the most comprehensive assessments of MBSE evidence, Henderson and Salado conducted a systematic literature review categorizing reported benefits into four evidence types: measured, observed, perceived, and referenced [78]. Their finding that approximately two-thirds of claimed MBSE benefits lack empirical measurement and instead rely upon perceived or referenced evidence carries profound implications for adoption decisions. Organizations evaluating MBSE investment discover that the research literature offers abundant testimony to MBSE's promise but limited quantified outcomes upon which to build business cases. Madni and Sievers reached a similar conclusion in their review of MBSE motivation and research opportunities, arguing that the value proposition requires demonstration through real-world applications and that further advancements remain necessary before broader adoption can occur [79]. More recently, Wooley and Womack analyzed adoption, benefits, and challenges across the Digital Engineering research corpus and explicitly noted the absence of research addressing enterprise IT infrastructure or Information Assurance applications [80]. Their finding validates that the research gap identified in this dissertation reflects the actual state of academic literature rather than incomplete literature search.

Among the rare exceptions to the measurement deficit, the work of Rogers and Mitchell stands as the most frequently cited quantified evidence of MBSE return on investment [25]. Their case study examined the Submarine Warfare Federated Tactical Systems program—a rapidly evolving combat system of systems comprising over ten million source lines of code deployed across 104 submarines—following a three million dollar MBSE investment over two and a half years. An apples-to-apples comparison between legacy document-centric processes and the MBSE approach revealed that systems engineering hours per requirement decreased from 12.1 to 9.9, representing an eighteen percent improvement in efficiency that exceeded the thirteen percent improvement projected by an earlier pilot study. The MBSE approach handled forty-two percent more interface requirements changes while consuming only sixteen percent more hours, reduced total interface defects

by nine percent, and shifted eighteen percent of defects to earlier discovery phases where correction costs between 1.6 and 4 times less than defects discovered during platform integration testing. Supplementary data demonstrated thirty percent more baselines produced monthly and sixty percent more integrated subsystems and combat system variants managed within constant resources.

Significant not merely for their magnitude but for their scarcity, these results merit careful examination. Henderson and Salado identified the Rogers and Mitchell study as one of only two papers in the literature reporting measured MBSE return on investment evidence [78]. As a practical consequence, organizations contemplating MBSE adoption must extrapolate from a remarkably thin evidence base. For enterprise IT organizations operating on annual budgets with continuous delivery expectations, this evidentiary deficit creates a rational basis for hesitation: the demonstrated benefits derive from a naval combat system program operating under a level-of-effort contract structure fundamentally different from enterprise IT budget models. Whether comparable returns would materialize in enterprise IT contexts remains entirely unexamined.

Earlier systematic reviews reinforce this pattern. Wolny et al. reviewed thirteen years of SysML research, mapping the landscape of model-based methods and their empirical evidence [81]. Chami and Bruel surveyed MBSE tools and applications, finding consistent reports of improved requirements traceability and stakeholder communication alongside persistent concerns about tool complexity and organizational adoption challenges [82]. 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 that limit realization of theoretical benefits [83]. Collectively, these reviews establish that MBSE has demonstrated value across multiple domains while simultaneously documenting two critical limitations: the evidence remains predominantly qualitative, and the domains of application remain overwhelmingly confined to aerospace and defense.

The tension between demonstrated capability and insufficient proof creates what might be termed an adoption credibility gap. Within the systems engineering discipline, professional experience and institutional knowledge compensate for the measurement deficit. Systems engineers who have used MBSE tools can observe improvements in their own work, creating the experiential validation that published evidence lacks. Outside the discipline, this compensatory mechanism does not operate. IT and Information Assurance professionals have no experiential basis for evaluating MBSE claims. The literature provides them with compelling arguments but insufficient evidence—a combination that technology adoption research suggests is inadequate for driving adoption decisions.

2.2 Adoption as a Perception Problem

If the evidence paradox explains why MBSE has not expanded through rational economic calculation, the adoption literature reveals a complementary explanation rooted in perception dynamics. A growing body of empirical research demonstrates that MBSE adoption decisions are driven more by how professionals perceive the technology than by its objective characteristics. This finding carries direct implications for the present research: if perceptions govern adoption even among systems engineering professionals who work with models daily, understanding perceptions among IT and Information Assurance professionals—who have never systematically encountered these methodologies—becomes a prerequisite for any meaningful discussion of cross-disciplinary transfer.

The theoretical foundation for this argument derives from Call and Herber, who mapped Everett Rogers' Diffusion of Innovations theory to MBSE adoption dynamics [84]. Rogers' framework identifies five perceived attributes of innovations—relative advantage, compatibility, complexity, trialability, and observability—that collectively account for forty-nine to eighty-seven percent of variance in adoption rates across innovation research. The critical theoretical insight, and the one most consequential for the present

research, is that *perceptions* of these attributes, not the attributes themselves, drive adoption behavior. Call and Herber invoke W. I. Thomas's dictum that "if [people] perceive situations as real, they are real in their consequences," arguing that shaping how MBSE attributes are perceived can accelerate adoption rates more effectively than improving the attributes themselves [84].

Call et al. tested this theoretical mapping empirically through a survey of approximately 270 systems engineering professionals distributed through INCOSE and professional networks [75]. Across six subpopulation comparisons—involved versus not involved in MBSE efforts, model users versus non-users, and respondents subject to Digital Engineering mandates versus those who are not—the study examined perceptions. Respondents broadly recognized MBSE's relative advantage in improving data quality and traceability. However, perceived compatibility with existing practices and perceived complexity emerged as significant barriers that suppressed adoption even when practitioners acknowledged objective value.

The most striking finding involves trialability. Respondents not involved in MBSE efforts reported dramatically lower access to trial opportunities and tools, with a chi-squared test result of $p = 0.00$ for the involved/non-involved comparison [75]. What Call et al. characterize as a barrier-reinforcing cycle emerges: professionals who have not experienced MBSE cannot access the trial opportunities that would facilitate informed adoption decisions, while those who have experienced MBSE report substantially more favorable perceptions. Further complicating adoption, the study characterizes MBSE as a "preventative innovation" whose advantages derive from preventing problems—inconsistencies, documentation errors, rework—rather than producing visible new benefits. Depressed perceived relative advantage and observability compound adoption barriers even when objective value exists.

This perception-adoption dynamic has profound implications for cross-disciplinary transfer. If systems engineering professionals—practitioners who work within the dis-

cipline that developed MBSE—exhibit perception gaps that impede adoption, the perception barriers among IT and Information Assurance professionals are likely to be substantially greater. These professionals operate outside the systems engineering discipline entirely. They have no professional exposure to MBSE concepts, no institutional networks sharing MBSE experiences, and no trial opportunities through which favorable perceptions might develop. The present research addresses this gap by measuring perceptions in a population where no empirical data currently exist.

Complementary evidence from Henderson et al. deepens understanding of adoption dynamics through a mixed-methods study combining systematic literature review with eighteen semi-structured practitioner interviews from organizations attempting MBSE adoption [74]. From the literature review, over six hundred individual lessons learned were extracted from forty-six published papers, coded into categories spanning communication, model definition, organizational strategy, and technical implementation. Interview findings illuminate the human dimensions of adoption that quantitative studies cannot fully capture. Perhaps most directly relevant to the question of professional awareness, approximately twenty-two percent of interview participants—all systems engineering professionals—could not convey a clear definition of MBSE. One participant captured the prevailing confusion: "Most people think of MBSE as being synonymous with a specific tool" and "don't understand how MBSE fits into DE or what it really does other than it is modeling instead of documents" [74]. Another stated plainly that "if they aren't familiar with MBSE, they're not going to use it."

The organizational lessons proved equally revealing. For both organizations in the study whose adoption efforts failed, the driving barrier was lack of management support. Middle management resistance proved particularly insidious because executives endorsed MBSE while middle managers could disregard the endorsement without operational consequences. Successful adopters commonly established core MBSE teams—communities of practice or centers of excellence—and implemented role-based training at four levels:

model reviewers for leaders and decision-makers, developers and modelers, architects for senior engineers, and administrators for IT and software support. A reinforcing dynamic emerged: greater stakeholder exposure to models produced more perceived benefits, which generated more organizational buy-in, which enabled further exposure. This virtuous cycle operates within organizations that have initiated adoption but cannot initiate itself in domains where MBSE has never been introduced.

Henderson and Salado extended these findings by examining how organizational structure variables correlate with MBSE adoption outcomes through a survey of fifty-one practitioners [85]. The results reveal a pattern with direct implications for enterprise IT contexts. Flexibility and interconnectedness showed the strongest and most consistent positive correlations with both adoption process and implementation variables. Formalization—documented procedures and processes—correlated positively, a somewhat counterintuitive finding suggesting that governance frameworks support rather than hinder adoption when combined with flexibility. Centralization correlated negatively with adoption and implementation, as did large organizational size and high vertical differentiation. These structural findings suggest that enterprise IT organizations characterized by rigid hierarchies, centralized governance, and siloed operations may face structural impediments to Digital Engineering adoption that compound the perception barriers documented by Call et al.

Research beyond the systems engineering discipline corroborates these dynamics. Vogelsang et al. conducted a qualitative study of twenty interviews across ten companies in the embedded systems industry—outside the defense and aerospace sector where MBSE originated [86]. Their findings identified immature tooling, return on investment uncertainty, and migration fears as key barriers, confirming that the adoption challenges documented within systems engineering intensify when the technology crosses disciplinary boundaries. Campagna et al. examined strategic adoption of digital innovations more broadly, finding that digital transformation requires coordinated enterprise-level applica-

tion rather than bottom-up adoption of individual technologies [87]. The research identified twelve strategic adoption influencers and noted that adoption research focuses upon individual technologies rather than integrated digital transformation—a finding that explains why platform-level Digital Engineering adoption within defense programs has not expanded to enterprise IT functions operating separately from program organizations.

The adoption literature thus establishes a critical precondition for the present research. Technology adoption is governed by perceptions. Perceptions among systems engineering professionals—the population most favorably positioned to appreciate MBSE—remain mixed and marked by significant awareness deficits. No comparable perception data exist for IT and Information Assurance professionals. Until such data are collected, any discussion of Digital Engineering adoption beyond defense and aerospace rests upon assumption rather than evidence. This dissertation addresses that evidentiary gap.

2.3 Crossing Disciplinary Boundaries: Digital Engineering Beyond Its Origins

Concentrated within aerospace and defense, Digital Engineering raises an unresolved question that the literature has acknowledged but not adequately investigated: can these methodologies transfer effectively to domains with different professional cultures, tool ecosystems, and economic structures? Preliminary evidence is suggestive but fragmented, consisting of isolated applications to security domains, a conceptual framework from an authoritative institution, and a single systematic mapping study of model-based security engineering. No sustained research program has examined cross-disciplinary transfer to enterprise IT or Information Assurance.

Bone et al. described the Systems Engineering Research Center's research effort underlying the DoD Digital Engineering initiative, identifying three key enablers for transformation: IT infrastructure, workforce development, and policy [88]. Though defense-

originated, their analysis addressed cross-cutting adoption dynamics and workforce transformation challenges applicable to any domain adopting Digital Engineering. The transformation they described requires coordinated investment across technology, people, and governance—precisely the integrated approach that enterprise IT organizations, structured around operational silos and annual budget cycles, struggle to sustain.

Perhaps the most substantive bridge between Digital Engineering and Information Assurance comes from the Carnegie Mellon Software Engineering Institute. Chick et al. argued that DevSecOps pipelines constitute complex socio-technical systems—comprising independently developed and maintained, physically and logically distributed, interoperable components—that require systems engineering treatment [77]. Tight integration of business mission, capability delivery, and products "increases the attack surface of the product under development," and as organizations adopt DevSecOps tools and techniques with increased coupling between products and the tools used to build them, "the attack surface continues to grow, incorporating segments of the development environment itself." The research developed a DevSecOps Platform Independent Model using the Unified Architecture Framework and SysML to model pipeline security properties, demonstrating how to construct cybersecurity assurance cases from model-based representations.

The SEI framework proposed a conceptual shift with direct relevance to this dissertation: from process-based to property-based security assurance. Traditional cybersecurity assurance relies upon process-based standards such as the NIST Risk Management Framework and SP 800-53 security controls. As systems become more complicated and interconnected, Chick et al. argued, "process-based standards fail to assure system owners that the system functions only as intended under all operational circumstances" [77]. When MBSE-based assurance is implemented effectively, "the overall risks associated with the DevSecOps pipeline and associated products will be reduced, and the compliance and legal requirements will naturally be addressed within the engineering lifecycle." This finding directly supports the theoretical premise of this dissertation: that Digital Engineering

capabilities can integrate security engineering into development and operational processes rather than treating compliance as a separate activity conducted after the fact.

However, the SEI framework represents a conceptual and architectural argument rather than empirical validation. Technical feasibility is demonstrated through detailed modeling of configuration management capabilities, but quantitative effectiveness data are absent. Designed for heavily regulated and cybersecurity-constrained environments including defense, banking, and healthcare—domains where Information Assurance professionals operate and where compliance verification demands consume substantial organizational resources—the framework leaves the critical question unanswered: does MBSE-based security assurance deliver measurable improvements over traditional compliance approaches in practice?

Other researchers have probed adjacent territory without directly addressing enterprise IT. Huff et al. developed an MBSE methodology for critical infrastructure vulnerability assessment and decision analysis, using DoDAF-based modeling to link regulatory requirements, system architecture, and attack vectors [89]. Their work demonstrates MBSE application to infrastructure protection and security assessment beyond traditional platform engineering but does not extend to enterprise IT infrastructure management. Mažeika and Butleris presented a UML-based MBSE security profile conforming to ISO/IEC 27001 and found through a feasibility survey of ten engineering companies that security aspects are inadequately addressed by standard SysML and popular MBSE methods [90]. A tool gap identified by this finding would impede adoption even if organizational and perception barriers were overcome: the modeling languages themselves require extension to accommodate security constructs that enterprise IT and Information Assurance demand. Apvrille and Roudier proposed SysML-SecA, combining SysML with security analysis techniques for integrated threat modeling [91]. Collectively, these preliminary investigations establish that researchers have recognized the potential of MBSE for security applications while simultaneously documenting the technical, methodological,

and empirical gaps that separate potential from realization.

Nguyen et al. conducted a systematic mapping of forty-eight primary studies on model-based security engineering for cyber-physical systems [92]. The study found that most research uses domain-specific languages or UML, focuses upon early lifecycle stages, and addresses threats, attacks, and vulnerabilities generically. This mapping reveals a field in its formative stages—one where foundational concepts are being established but where mature, validated methodologies for operational security engineering have not yet emerged. The gap between model-based security engineering research and operational Information Assurance practice remains substantial.

The academic literature on MBSE applications thus presents a landscape of expanding interest constrained by limited evidence. Researchers have begun exploring applications to security domains, infrastructure protection, and compliance frameworks. Authoritative institutions have produced conceptual frameworks demonstrating technical feasibility. Yet the enterprise IT context—where organizations manage heterogeneous infrastructure, maintain compliance across multiple regulatory frameworks, and coordinate service delivery across organizational silos—remains conspicuously absent from the research. 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.

2.4 Digital Twins as Emerging Security Tools

Digital twin technology has generated substantial research interest in cybersecurity applications, creating a parallel track to MBSE-based security engineering that the literature has not yet integrated into a coherent Digital Engineering narrative. The growing body of research on digital twins for security purposes represents both an opportunity and an analytical challenge: it demonstrates that Digital Engineering concepts are penetrat-

ing security domains, but it does so through a technology-specific lens that misses the integrated approach—combining MBSE, digital threads, digital twins, and PLM—that characterizes Digital Engineering as a discipline.

Grieves traces the evolution of digital twin concepts from Product Lifecycle Management origins through contemporary applications, positioning digital twins as the integration of physical and virtual systems that enables analysis, optimization, and prediction [39]. The foundational distinction between digital twins and traditional simulation lies in synchronization: digital twins maintain continuous data exchange with their physical or logical counterparts, enabling operational decision-making based upon current rather than documented system states. Madni and Sievers provided an influential framework for leveraging digital twins in systems engineering contexts, establishing the conceptual architecture that subsequent security applications adapted [37].

El-Hajj et al. conducted a systematic literature review analyzing sixty-seven papers published between 2018 and 2023 examining how digital twins enhance security in Industry 4.0 applications [93]. Covering intrusion detection, vulnerability assessment, cyber range simulation, and threat intelligence applications, the review identified enabling technologies—machine learning, blockchain, and 5G—used in conjunction with digital twins for security purposes. Alhumam et al. extended this analysis in a comprehensive review categorizing digital twin cybersecurity studies by technique type and digital twin level—component, process, asset, system, and network-of-systems—assessing risk levels from medium to very high depending upon twin type and industry sector [94]. Collectively, these systematic reviews confirm that digital twin security applications have achieved sufficient research volume to warrant meta-analysis, indicating a maturing research area.

Within this expanding literature, several streams bear directly upon Information Assurance and enterprise IT applications. Eckhart and Ekelhart reviewed digital twins for cyber-physical systems security, examining how virtual replicas can support security testing and analysis without affecting operational systems [95]. Vielberth et al. pro-

posed a digital twin-based cyber range for Security Operations Center analyst training, demonstrating practical application of digital twin concepts to security workforce development [96]. Dietz and Pernul examined digital twins for enterprise security, exploring how organizations might employ virtual representations to understand and manage security postures [97]. Karaarslan and Babiker examined digital twin security threats and countermeasures, addressing the bidirectional security challenge: digital twins can enhance security while simultaneously introducing new attack surfaces [98].

Standards development further indicates maturing technology readiness. Shao examined ISO 23247 and IEC 62832 standards for digital twin frameworks [36]. Shao et al. provided additional analysis of ISO 23247's four-part structure [41]. The Internet Engineering Task Force has published a draft reference architecture for network infrastructure digital twins [42]. Together, these standardization efforts establish interoperability requirements that reduce vendor lock-in concerns and enable integration across implementations.

NIST's engagement with digital twin technology illuminates the current state of institutional thinking. NIST Internal Report 8356 addresses cybersecurity challenges and trust considerations for digital twin implementations [43]. Significantly, this publication addresses security considerations *for* systems employing digital twins rather than digital twin applications *to* Information Assurance. A revealing distinction emerges: NIST examines how to secure digital twin implementations rather than how digital twins might enhance security posture visibility or compliance verification. Current institutional research thus frames digital twins as systems to be secured rather than as tools for improving security operations.

Academic research on open source digital twin frameworks adds another dimension to the adoption question. Gil et al. conducted a systematic survey of open source digital twin frameworks, analyzing fourteen frameworks against criteria derived from ISO 23247 standards and finding significant variation in maturity, documentation quality, and community support [48]. Autiosalo et al. introduced Twinbase, an open source server for the

Digital Twin Web concept [49]. While these open source options reduce economic barriers to adoption, they do not resolve the more fundamental challenge: digital twin applications for enterprise IT contexts lack the academic research and validated methodologies that would guide adoption decisions.

However, framing digital twins exclusively as defensive or simulation tools obscures a critical dimension of the technology: the bidirectional data streams that enable digital twin functionality simultaneously constitute primary attack surfaces. Alcaraz and Lopez conducted the most comprehensive survey of digital twin security threats to date, classifying attack vectors across both digital and physical layers and cataloging threats including software exploitation, privilege escalation, denial of service, data extraction, and man-in-the-middle attacks targeting the communication channel between physical systems and their virtual counterparts [99]. Their analysis demonstrates that adversaries who compromise a digital twin can extract private information—including services, dynamics data, configurations, states, and security credentials—that may subsequently be weaponized for cyber espionage or leveraged to identify and exploit vulnerabilities in production systems. Attacks cascade bidirectionally: compromise of the digital representation can propagate to physical systems, while manipulation of physical components can corrupt digital twin fidelity.

Suhail et al. confronted the assumption that digital twins serve purely security-enhancing functions, introducing the concept of malicious digital twins that adversaries can exploit as observation platforms to covertly learn physical system behavior through model analysis [100]. Their analysis identifies a fundamental tension: high-fidelity digital twins required for accurate security analysis simultaneously create high-fidelity attack surfaces from which adversaries can extract operational intelligence. Malicious actors can interrupt digital threads connecting physical counterparts, cause information leakage exposing system functioning, and manipulate physical operations through compromised twin interfaces. In a related investigation, Suhail et al. documented a two-stage adversary strategy

in which attackers first place the digital twin into a malicious state as a data acquisition source, then exploit that compromised state to covertly manipulate the underlying physical system [101]. Cyclic state updates between the twin and the physical process amplify the potential for cascading damage.

At the infrastructure level, the communication layer connecting physical and digital twins represents the most concentrated attack surface. Rodrigues et al. identified the data connection layer as the central nervous system of digital twin architecture in Industry 4.0 environments and demonstrated that denial-of-service, man-in-the-middle, and intrusion attacks targeting bidirectional data streams via OPC UA and MQTT channels can corrupt twin fidelity and trigger hazardous actions in physical systems [102]. Their proposed data rate monitoring approach achieved complete detection across all three attack categories, but the underlying finding carries broader significance: the IT/OT convergence that digital twins facilitate introduces security challenges distinct from traditional IT environments, including resource-constrained devices, heterogeneous protocols, and legacy system integration requirements. Gehrmann and Gunnarsson reached a complementary conclusion, demonstrating that opening industrial automation and control system functions through digital twin interfaces creates threat vectors for which traditional ICS security approaches prove insufficient [103]. Eckhart et al. systematized security-enhancing digital twins while acknowledging that twins accurately reflecting physical devices—including their vulnerabilities—simultaneously create information assets that adversaries could exploit, and that digital twins deployed as honeypots face the paradox of providing adversaries with detailed knowledge of real system behavior [104].

These findings carry direct implications for the present research. Organizations contemplating digital twin adoption for Information Assurance purposes must address a dual challenge: securing the digital twin implementation itself while leveraging its capabilities for security improvement. Digital twins that provide visibility into system configurations, dependencies, and security postures also concentrate precisely the information that adver-

saries seek. Appropriate protections must ensure that threat actors cannot compromise the digital twin or extract knowledge from it that could be used to exploit production environments. NIST's framing of digital twins primarily as systems requiring security—rather than as security tools—reflects institutional recognition of this duality, even if the research community has not yet developed comprehensive frameworks for managing the tension between digital twin utility and digital twin vulnerability in enterprise contexts.

The digital twin security literature thus reveals a field developing in parallel with but largely disconnected from the broader Digital Engineering discourse. Researchers explore digital twins as security tools without embedding their work within the Digital Engineering framework that integrates MBSE, digital threads, and PLM into a coherent discipline. This disconnection means that individual digital twin security capabilities are investigated in isolation rather than as components of the integrated approach that defense and aerospace organizations employ. Whether integrating digital twin security capabilities within a comprehensive Digital Engineering framework would produce greater value than isolated implementations remains an open question—one that the absence of enterprise IT research leaves entirely unaddressed.

2.5 The Compliance Imperative and Its Unfulfilled Requirements

Compliance frameworks create requirements that Digital Engineering could address, yet no research examines Digital Engineering approaches to satisfying these requirements. This disconnect between what frameworks demand and what current practices deliver represents one of the most compelling arguments for investigating Digital Engineering application to Information Assurance.

Documented in Special Publication 800-37 Revision 2, the NIST Risk Management Framework provides the authoritative approach to managing security and privacy risk

for federal information systems through seven iterative steps: prepare, categorize, select, implement, assess, authorize, and monitor [105]. Critically, the RMF explicitly requires enterprise architecture integration 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. NIST Special Publication 800-53 Revision 5 compounds these demands through specific controls requiring 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 [4]. Each control establishes compliance obligations that Digital Engineering could address. Yet no research examines Digital Engineering approaches to satisfying these specific controls.

The Committee on National Security Systems Instruction 1253 extends these requirements to national security systems, where documentation and visibility challenges compound under additional constraints [106]. Organizations operating outside federal requirements may employ ISO/IEC 27001:2022 for information security management [12]. Mažeika and Butleris found that standard MBSE methods inadequately address ISO 27001 security requirements, identifying a specific gap between what compliance frameworks demand and what current modeling approaches provide [90]. These alternative frameworks share a common characteristic with NIST guidance: they assume documentation accuracy and visibility capabilities that organizations struggle to maintain.

Beyond federal information systems and national security systems, an expanding compliance landscape governs nonfederal organizations that process, store, or transmit Controlled Unclassified Information (CUI) on behalf of government agencies. NIST Special Publication 800-171 Revision 3 establishes security requirements for protecting CUI in nonfederal systems and organizations [14]. Revision 3, finalized in May 2024, restruc-

tured the framework from fourteen to seventeen security requirement families—adding Planning, System and Services Acquisition, and Supply Chain Risk Management—while reducing individual requirements from 110 to 97 but increasing the specificity of each requirement to 266 individual control items. Significantly, Revision 3 aligned its control structure directly with SP 800-53 Revision 5 as the single authoritative source and introduced forty-nine Organization-Defined Parameters that provide implementation flexibility while enabling automated compliance assessment through machine-readable formats such as OSCAL. SP 800-171's architecture is substantially more amenable to automation than its predecessor, and the closer alignment with SP 800-53 enables organizations to leverage common tooling across federal and nonfederal compliance obligations.

NIST Special Publication 800-172 supplements the SP 800-171 baseline with thirty-five enhanced security requirements designed to protect CUI associated with critical programs and high-value assets against Advanced Persistent Threats [16]. SP 800-172 operates upon a three-pillar defense strategy: penetration-resistant architecture, damage-limiting operations, and cyber resiliency and survivability. Enhanced requirements span access control, configuration management, identification and authentication, incident response, risk assessment, situational awareness, and system protection—each demanding capabilities that manual processes and static documentation struggle to sustain at the required tempo. Federal agencies select applicable requirements based upon mission needs and risk assessment, creating a tailored compliance burden that automated, model-based approaches could reduce. A Revision 3 update currently in development expands scope from confidentiality protection alone to encompass confidentiality, integrity, and availability, further increasing the documentation and verification demands upon implementing organizations.

The Cybersecurity Maturity Model Certification (CMMC) 2.0 framework operationalizes these NIST requirements within the Department of War's defense industrial base through a three-tiered certification structure [17]. Level 1 requires fifteen foundational practices for Federal Contract Information protection through annual self-assessment.

Level 2 mandates compliance with the 110 requirements of SP 800-171 Revision 2, assessed through triennial third-party evaluation by CMMC Third-Party Assessment Organizations (C3PAOs). Level 3 adds twenty-four enhanced requirements drawn from SP 800-172, assessed by the Defense Industrial Base Cybersecurity Assessment Center. Phase 1 implementation commenced in November 2025, with full implementation across all contracts involving Federal Contract Information or Controlled Unclassified Information expected by November 2028. CMMC represents a fundamental shift from self-attestation to verified compliance, imposing documentation and evidence requirements that intensify the challenges organizations already face in maintaining accurate, current security documentation.

The intersection of these compliance frameworks with emerging technologies—particularly artificial intelligence, DevSecOps automation, and continuous monitoring—has received limited but growing academic attention. Haverinen et al. proposed an approach for automating cybersecurity compliance management within DevSecOps pipelines through an open information model that encodes compliance requirements as logic programs, enabling automated policy checks and compliance calculations [107]. Their framework-agnostic approach demonstrates technical feasibility of encoding NIST-aligned controls as code—a capability that digital threads could extend by connecting compliance-as-code implementations to authoritative system models. NIST's own DevSecOps guidance, including SP 800-204D on software supply chain security integration within CI/CD pipelines [108], establishes institutional expectations for automated security within development and operational workflows. Yet the academic literature connecting CMMC compliance automation to Digital Engineering remains sparse. The near-absence of peer-reviewed research at this intersection—despite growing practitioner interest and institutional investment—reinforces the contribution of the present investigation: understanding whether Information Assurance professionals perceive value in Digital Engineering capabilities that could address the documentation, traceability, and verification demands these compliance

frameworks impose.

NIST's systems security engineering publications establish principles that align with Digital Engineering's integrated approach. Special Publication 800-160 Volume 1 Revision 1 describes a basis for engineering trustworthy secure systems [50]. Special Publication 800-160 Volume 2 Revision 1 addresses cyber resiliency considerations [58]. While these publications reference model-based approaches and traceability requirements, they do not provide specific implementation guidance for Digital Engineering in enterprise IT contexts. Requirements that Digital Engineering could address are established—traceability between security requirements, design decisions, and implementation artifacts; documentation that maintains currency throughout system lifecycles; visibility into system configurations and relationships—yet they do not explicitly connect these requirements to Digital Engineering solutions.

Emerging research on compliance automation demonstrates that the academic community has recognized the inadequacy of manual compliance approaches, even if this recognition has not yet connected to the Digital Engineering discourse. Joshi et al. developed a semantically rich knowledge graph capturing regulations from GDPR, PCI DSS, ISO 27001, NIST 800-53, and CSA CCM, enabling automated compliance checking for cloud services [109]. Their work, validated against privacy policies of major cloud providers, demonstrates that model-based approaches to compliance are technically feasible and practically valuable. Banse et al. presented the Cloud Property Graph, bridging static code analysis and runtime security assessment using an ontology of cloud resources to enable automated identification of misconfigurations and regulatory non-compliance across multi-vendor cloud deployments [110]. Stojkov et al. proposed a UML-based model for cross-standard security requirements with explicit mapping to NIST's Open Security Controls Assessment Language (OSCAL) Catalog Model, enabling organizations to track compliance across multiple frameworks simultaneously [111]. Most recently, Koufos et al. combined attack graphs with OSCAL using compliance-as-code principles to automate

risk assessment [112].

NIST's own OSCAL initiative represents institutional recognition that manual documentation approaches cannot sustain the accuracy and currency that compliance requires [15]. OSCAL provides standardized machine-readable formats for expressing security control catalogs, baselines, profiles, and assessment results. The initiative aligns with Digital Engineering's emphasis upon machine-readable documentation, and digital thread traceability could connect OSCAL compliance documentation to underlying system configurations, enabling automated verification that documented controls exist as implemented. Yet this integration has not been investigated in the academic literature.

The compliance automation research and the Digital Engineering literature thus develop along parallel tracks that have not converged. Compliance researchers build knowledge graphs, property graphs, and domain-specific languages to automate regulatory assessment. Digital Engineering researchers develop model-based approaches, digital threads, and authoritative sources of truth for complex system management. Both communities address documentation accuracy, traceability, and automated verification. Neither community has systematically explored how integrating their approaches might produce capabilities exceeding what either achieves independently. This unexplored intersection represents a significant research opportunity that the present investigation begins to address by establishing whether the professionals who must implement compliance—IT and Information Assurance practitioners—recognize value in Digital Engineering capabilities.

DevSecOps literature provides additional context for this compliance discussion. Rajapakse et al. conducted a systematic review of fifty-four peer-reviewed studies identifying twenty-one challenges and thirty-one solutions in DevSecOps adoption, classified into People, Practices, Tools, and Infrastructure themes [113]. Recommending shift-left security and continuous security assessment, the review identified approaches that align conceptually with the integrated security engineering that MBSE enables. Earlier, Myrbakken

and Colomo-Palacios provided one of the first systematic examinations of DevSecOps, defining the field and characterizing the challenges of integrating security into DevOps practices [114]. These DevSecOps studies establish the problem space—integrating security into development and operational pipelines—without connecting to the Digital Engineering framework that could provide structured methodology for that integration.

2.6 IT Service Management: Structural Failures Despite Mature Frameworks

IT Service Management frameworks assume capabilities that current practices cannot sustain. The Information Technology Infrastructure Library provides comprehensive guidance for aligning IT services with business needs through structured processes, yet ITIL's effectiveness depends upon the accuracy and currency of underlying configuration information—accuracy that organizations consistently fail to achieve [5]. ITIL 4 reorganized service management practices and introduced the Service Value System concept, acknowledging that tracking configurations across virtual systems, cloud computing, and cybersecurity domains presents challenges, but providing limited guidance on addressing the documentation accuracy challenges that undermine every ITIL process [115].

Empirical evidence for ITIL implementation challenges proves revealing. Cook et al. found resistance to change at twenty-seven percent as the top ITIL implementation challenge [116]. Marrone and Kolbe surveyed 491 firms finding that while over ninety percent use ITSM frameworks, little research examines actual benefits realized [117]. A striking parallel with MBSE evidence emerges: both MBSE and ITIL are widely adopted based upon perceived rather than measured value, and both face adoption challenges rooted in organizational factors rather than technical limitations. Yet no research examines whether integrating Digital Engineering practices with ITIL frameworks could address the persistent challenges that ITIL alone has not resolved.

Configuration Management Database failures provide the most extensively documented evidence of structural inadequacy. Gartner reports an eighty percent failure rate for CMDB implementations [18]. Additional research indicates that ninety-nine percent of organizations using CMDB tooling without addressing data quality gaps will experience visible business disruption [118]. Forrester research finds that less than half of organizations trust the data in their CMDB [119]. Peer-reviewed research corroborates these industry findings: Hauder et al. found through a study of 123 enterprise architecture practitioners that manual documentation processes cannot maintain accuracy in dynamic environments [120]. Data quality statistics reveal the core challenge: sixty percent of data manually input by employees proves inaccurate [121].

Recent analysis concludes that the CMDB approach itself has failed [122]. After decades of implementation attempts across organizations, CMDBs consistently fail to deliver intended value. Failure attribution centers upon structural issues: involving process experts rather than data management professionals, manual data entry that cannot maintain accuracy, and scope creep that renders CMDBs unmanageable. 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 [123]. Such findings suggest that incremental CMDB improvements cannot resolve inherent approach limitations—a conclusion that opens conceptual space for model-based alternatives that maintain accuracy through automated synchronization rather than manual data entry.

Shadow IT compounds the documentation challenge. Gartner research indicates forty-one percent of employees used shadow IT in 2022, expected to climb to seventy-five percent by 2027, with thirty to forty percent of large companies' IT expenditure representing shadow IT [20]. Klotz et al. conducted a systematic review of 126 publications documenting how silos between business units and IT departments drive shadow IT, creating security risks, data inconsistency, and compliance violations [124]. Systems deployed

outside formal governance remain invisible to IT operations and security teams, creating unknown attack surfaces that no documentation process can capture. Fürstenau et al. examined organizational dynamics when hidden IT systems are discovered, revealing interdepartmental conflicts and governance failures that perpetuate documentation gaps [125]. Shadow IT reflects a structural mismatch between IT governance and organizational needs: when official IT processes cannot meet user requirements quickly enough, users acquire solutions independently, creating operational dependencies that official documentation does not capture.

Change management effectiveness depends directly upon documentation accuracy. Industry analysis confirms that reliance upon outdated documentation leads to inaccurate impact assessments [126]. Research by Bokan and Santos highlights difficulties organizations encounter in maintaining comprehensive security oversight [8]. Change management depends upon accurate understanding of system relationships [127] that current documentation approaches cannot maintain. 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 that consume resources, damage trust in change processes, and create pressure for emergency changes that further degrade documentation accuracy. A self-reinforcing cycle emerges, resistant to process improvement within the document-centric paradigm.

Thompson et al. examined integrating MBSE with IT Service Management, and previous research by Bonar and Hastings demonstrated that compliance verification is enhanced by Digital Engineering practices [76], [128]. These preliminary investigations suggest that integration between Digital Engineering and IT Service Management offers value, though comprehensive research remains absent.

2.7 Enterprise Visibility: Empirical Evidence of Systemic Failure

Challenges documented in the preceding sections share common roots in the inability of organizations to maintain accurate, current documentation of their enterprise information systems. Synthesizing peer-reviewed research and industry analysis, this section establishes that these challenges reflect systemic patterns rather than isolated organizational deficiencies, and to provide the empirical foundation for evaluating Digital Engineering as a potential disciplinary response.

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 [19]. Ponemon Institute's 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 [129]. Only fifteen percent of respondents in the SANS Institute SOC Survey expressed very high confidence that all devices on their network are discoverable [130]. Compounding across organizational boundaries, these visibility gaps Ivanti's 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 [131]. The Cloud Security Alliance revealed that ninety-five percent of organizations suffered cloud-related breaches in the preceding eighteen months [132]. Check Point 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 [133].

Peer-reviewed research provides empirical grounding for these industry findings. Yin et al. conducted an empirical study examining configuration errors in commercial and open source systems, finding that seventy to eighty-five percent of misconfigurations result from

mistakes in setting configuration parameters and that twenty-two to fifty-seven percent of misconfigurations involve configurations external to the examined system [134]. NIST Special Publication 800-128 defines configuration drift as systems deviating from baseline configurations over time through manual interventions, software updates, and environmental factors [135]. Uptime Institute's Annual Outage Analysis confirms that sixty-four percent of IT system outages occurred because of configuration or change management issues [136]. Complementing this finding, the IT Process Institute established that eighty percent of unplanned outages result from ill-planned changes made by administrators or developers [137]—changes that proper dependency documentation would have flagged.

Breach detection times serve as proxy measures for organizational visibility. 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 [21]. A 2025 update found that thirty-five percent of breaches involved shadow data—information stored in unmanaged locations—and forty percent involved data stored across multiple environments that organizations struggle to inventory comprehensively [138]. Taken together, these findings demonstrate that visibility failures directly impact security outcomes in measurable economic terms.

Peer-reviewed research provides theoretical and empirical frameworks for understanding why these failures persist. Bento et al. conducted a scoping review of forty studies on organizational silos, identifying five conceptualizations and characterizing silo mentality as an absence of systems thinking and organizational vision [139]. Beese et al. demonstrated through PLS-SEM analysis of 249 information systems managers that IS architecture complexity significantly reduces efficiency, flexibility, transparency, and predictability, and that organizations without adequate enterprise architecture management face compounding architectural degradation [140]. Kotusev examined twenty-seven organizations and found that prescribed enterprise architecture artifact lists from frameworks like TOGAF were never empirically validated and do not reflect actual practice—documenting

a fundamental gap between what frameworks recommend and what organizations find useful [141]. Kurnia et al. identified inhibitors to stakeholder engagement in enterprise architecture practice, including organizational silos, political barriers, and poor cross-team communication that directly undermine documentation quality and IT governance effectiveness [142]. Brée and Karger conducted a systematic literature review organizing enterprise architecture management challenges into six dimensions, with documentation challenges including dearth of automated tools, immature documentation models, and insufficient emphasis on forward-looking documentation [143].

Complexity theory provides an explanatory framework for why traditional documentation approaches fail in modern enterprise environments. Benbya and McKelvey applied Complex Adaptive Systems theory to information systems development, proposing seven first principles of adaptive success and arguing that if complexity is not managed appropriately, information systems fail [144]. Benbya et al. demonstrated that enterprise information systems have reached complexity levels exceeding prior technological generations [7]. 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—that static documentation approaches assume remain stable between documentation updates.

Technical debt research adds further perspective. Mendes et al. specifically addressed documentation technical debt—problems concerning non-existent, inadequate, or incomplete software project documentation [145]. Li et al. conducted a systematic mapping study covering ninety-four studies establishing technical debt taxonomy and management frameworks, including documentation debt as a distinct category [146]. Junior and Travassos consolidated perspectives on technical debt across nineteen secondary studies [147]. Kleinwaks extended technical debt concepts to systems engineering contexts [148]. Documentation technical debt accumulates when organizations defer documentation updates to prioritize operational activities. Unlike code technical debt, documentation debt re-

mains invisible until documentation is needed for change impact assessment, incident response, or compliance verification—at which point the accumulated debt imposes costs far exceeding the original deferral savings.

Table 2.1 summarizes the evidence documenting enterprise visibility and documentation failures across peer-reviewed and industry research sources.

Table 2.1: Enterprise Visibility and Documentation Failure Evidence

Finding	**Statistic**	**Source**
Visibility Gap Metrics		
IT environment monitorable	66%	IDC/Exabeam 2023[19]
Security teams lacking device visibility	63%	Ponemon Institute 2023[129]
High confidence in device discovery	15%	SANS Institute 2023[130]
Organizations with security/IT silos	55%	Ivanti 2025[131]
Configuration Management Failures		
CMDB implementation failure rate	80%	Gartner Research[18], [118]
Outages from configuration issues	64%	Uptime Institute 2023[136]
Misconfigurations from parameter errors	70-85%	Yin et al. 2011[134]
Unplanned outages from ill-planned changes	80%	IT Process Institute[137]
Shadow IT and Undocumented Assets		
Shadow IT as percentage of IT spend	30-40%	Gartner Research[20]
Cloud services vs. IT estimates	15-22x higher	Cisco 2016[149]
Employees using shadow IT (2022)	41%	Gartner Research[20]
Projected shadow IT usage (2027)	75%	Gartner Research[20]
Security Impact Metrics		
Mean time to identify breach	204 days	IBM/Ponemon 2024[21]
Cloud breaches from misconfigurations	82%	Check Point 2024[133]
Organizations with cloud breaches (18 mo)	95%	CSA 2024[132]
Projected preventable cloud breaches (2027)	99%	Gartner Research[150]

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.

A methodological observation regarding the evidentiary sources presented in this section warrants acknowledgment. Enterprise visibility evidence draws substantially upon industry analyst reports and practitioner surveys alongside peer-reviewed academic research. Reliance upon industry gray literature reflects a characteristic of the research domain rather than an analytical preference: the operational challenges of enterprise IT documentation and visibility have received considerably more attention from industry analysts and practitioner communities than from academic researchers. Relative scarcity of peer-reviewed empirical studies quantifying CMDB failure rates, shadow IT prevalence, and breach detection timelines itself constitutes evidence of the research gap this dissertation addresses. Where peer-reviewed evidence corroborates industry findings—as with the work of Hauder et al. on documentation accuracy, Mendes et al. on documentation technical debt, Beese et al. on architecture complexity, and Kotusev on enterprise architecture practice—the convergence strengthens confidence in the broader pattern. The industry evidence is presented not as a substitute for academic rigor but as the best available evidence for phenomena that academic research has not yet systematically investigated.

2.8 Research Gaps and Theoretical Framework

A clear pattern emerges from the systematic literature review: frameworks and compliance requirements assume documentation and visibility capabilities that organizations demonstrably lack, while Digital Engineering methodologies that could address these capabilities remain confined within a discipline that enterprise IT and Information Assurance have not engaged. Synthesizing the findings into a theoretical framework, this section documents the research gaps that this investigation begins to address.

The academic research gap is pronounced. Systematic literature reviews examining MBSE consistently find no research addressing enterprise IT infrastructure or Information Assurance applications beyond the preliminary reference model by Bonar and Hastings [76] and the conceptual DevSecOps framework by Chick et al. [77]. Persistence of this gap despite explicit requirements in compliance frameworks for capabilities that Digital Engineering provides demands explanation. Digital Engineering immaturity cannot account for it—defense and aerospace have employed Digital Engineering successfully for years. Tool unavailability cannot account for it—MBSE tools, digital twin platforms, and PLM systems have existed for over a decade (MBSE) to decades (digital twin, PLM, & authoritative traceability). Rather, the gap reflects a disciplinary boundary: systems engineering and IT have evolved as separate disciplines with limited cross-pollination, creating what Henderson and Salado would characterize as low interconnectedness between organizational units—precisely the structural condition their research associates with impeded adoption [85].

Standards bodies have recognized enterprise applicability of systems engineering approaches. The Unified Architecture Framework 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 standards-research disconnect leaves practitioners without empirical guidance for applying available standards to enterprise IT challenges.

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

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. Positing that Digital Engineering represents a disciplinary approach with demonstrated value in defense and aerospace contexts whose

Table 2.2: Research Gaps Within Corpus of Knowledge

Domain	**Gap Description**	**Research Implication**
MBSE for Enterprise IT	One study applying MBSE to enterprise IT, none for IA program management	Foundation research required
MBSE Adoption Evidence	Adoption studies limited to SE populations; no data from IT or IA professionals	Perception measurement needed in new populations
Digital Threads	No research on traceability for IT/IA contexts	Conceptual validation needed
Digital Twin	Growing security application research but no enterprise IT integration studies	Application studies needed
ITSM Integration	No frameworks integrating DE with ITIL	Integration research required
Compliance Automation	Model-based compliance research and DE research develop on parallel tracks without convergence	Integration research needed
Open Source	No academic validation for enterprise IT	Evaluation research needed
Professional Perceptions	Unknown awareness and perceived value among IT/IA professionals	This research addresses

capabilities align with gaps that have persisted in enterprise IT despite decades of framework development and organizational investment, this framework does not assert that Digital Engineering will resolve these gaps in enterprise IT contexts—that remains an empirical question. Rather, it identifies structural correspondences between demonstrated Digital Engineering capabilities and documented enterprise IT challenges, establishing the theoretical basis for investigating whether practitioners recognize these correspondences.

The persistent failures documented in IT Service Management and Information Assurance practices share common root causes that Digital Engineering practices are designed to 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. Digital Engineering's demonstrated ability to address these root causes in defense and aerospace contexts motivates investigation of whether similar benefits may transfer to enterprise IT environments.

The DoD Digital Engineering Strategy defines the authoritative source of truth as "a single source of data and models" that provides "a definitive technical baseline" for programs [3]. Current IT and Information Assurance practices lack authoritative sources of truth, instead maintaining multiple disconnected documentation artifacts that diverge over time. Digital threads establish and maintain authoritative traceability throughout system lifecycles, addressing the gap between security requirements, control implementations, and compliance evidence. Digital twin capabilities enable organizations to simulate system behavior, test proposed changes, and analyze scenarios without affecting production systems. Model-based approaches maintain synchronization with operational systems, providing the visibility that manual documentation cannot sustain.

The theoretical framework acknowledges several limitations. First, it extrapolates from Digital Engineering value demonstrated in aerospace and defense to anticipated value in

enterprise IT contexts. Whether benefits demonstrated for physical systems transfer to logical information systems remains unvalidated. Second, it assumes that Digital Engineering tools and methodologies can be adapted for enterprise IT contexts. Mažeika and Butleris documented that current MBSE methods inadequately address security requirements [90], suggesting adaptation requirements may exceed anticipated effort. Third, the framework does not address organizational change management, workforce development, or cultural transformation requirements. The adoption barriers documented by Henderson et al.—including middle management resistance, awareness deficits, and the need for dedicated MBSE teams [74]—would likely manifest with greater intensity in domains unfamiliar with systems engineering practices. 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.

2.9 Chapter Summary

This literature review has examined the current body of knowledge across interconnected domains relevant to applying Digital Engineering methodologies to Information Assurance and IT Service Management, advancing three interrelated arguments that position the present research within the academic conversation.

First, the evidence base for MBSE value, while compelling in individual cases such as the eighteen percent efficiency improvement and nine percent defect reduction documented by Rogers and Mitchell [25], remains disproportionately reliant upon perceived rather than measured outcomes. Henderson and Salado found that approximately two-thirds of claimed benefits lack empirical measurement [78]. This evidence deficit creates rational hesitation among organizations outside the systems engineering discipline, where institutional experience cannot compensate for the measurement gap.

Second, adoption research demonstrates that perceptions govern adoption decisions

more powerfully than objective technical merit. Call et al. showed that perceived complexity and compatibility barriers impede adoption even among systems engineering professionals who recognize MBSE's relative advantage [75]. Henderson et al. found that twenty-two percent of systems engineering professionals cannot clearly define MBSE [74]. If awareness deficits and perception barriers persist within the originating discipline, their magnitude among IT and Information Assurance professionals—who operate outside the systems engineering discipline entirely—demands empirical measurement rather than assumption.

Third, compliance frameworks and IT service management standards require capabilities that current practices demonstrably fail to provide, while Digital Engineering offers those capabilities in adjacent domains. Enterprise visibility evidence—sixty-six percent IT environment monitoring, eighty percent CMDB failure rates, 204-day average breach detection times—documents the scope of failure. Growing recognition within the compliance automation literature demonstrates that model-based approaches can address documentation and traceability requirements. Yet no research connects these parallel tracks by examining Digital Engineering as an integrated solution for enterprise IT and Information Assurance challenges.

Developed from this synthesis, the theoretical framework posits that structural correspondences between demonstrated Digital Engineering capabilities and documented enterprise IT challenges warrant investigation of whether practitioners recognize these correspondences. Contributing by investigating whether IT and Information Assurance professionals perceive value in Digital Engineering capabilities, the research. 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.

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.

Chapter 3

Research Methodology

This chapter presents the research methodology employed to investigate professional awareness and perceptions of Digital Engineering capabilities within the information technology and information assurance domains. Deploying a quantitative survey-based approach to collect data from IT and information assurance professionals, the study enables systematic analysis of awareness levels, perceived value, and anticipated benefits of Digital Engineering practices for information assurance and IT service delivery. Following a systems engineering lifecycle approach, the methodology itself demonstrates the application of structured engineering principles to research design while ensuring rigorous traceability between research questions, survey instruments, and analytical approaches.

3.1 Research Design Overview

This research employs a quantitative, cross-sectional survey design to address the three research questions established in Chapter 1. Survey methodology was selected as the most appropriate approach for several reasons. First, the research questions focus upon measuring professional awareness and perceptions across a broad population of IT and information assurance practitioners, requiring data collection from a number of respondents sufficient to establish representative findings. Second, survey methodology enables standardized data collection that supports statistical analysis and generalization of results

to the broader professional population. Third, the anonymous nature of survey research encourages candid responses about professional knowledge gaps and organizational capabilities without concerns about professional reputation or organizational disclosure. Practitioners can speak freely about what they do not know.

The cross-sectional design captures professional perceptions at a single point in time, providing a snapshot of current awareness and perceived value of Digital Engineering capabilities within the IT and information assurance professional community. While this design does not enable longitudinal analysis of changing perceptions over time, it establishes baseline data that shall inform future research directions and support strategic decision-making about Digital Engineering adoption initiatives.

3.1.1 Justification for Survey Methodology

The selection of survey methodology over alternative research approaches reflects deliberate consideration of what this research seeks to accomplish and why that objective warrants investigation. Three questions merit explicit address: why investigate perceptions rather than implementations, why survey methodology rather than case study or pilot implementation, and why perceived value warrants dissertation-level research.

3.1.1.1 Why Perceptions Matter for Technology Adoption

Technology adoption research consistently demonstrates that perceived value influences adoption decisions regardless of demonstrated actual value. The Technology Acceptance Model and its extensions establish that perceived usefulness and perceived ease of use predict behavioral intention to adopt technologies. Professionals who do not perceive value in a capability will not advocate for its adoption within their organizations, regardless of technical merit demonstrated in other contexts. The literature review in Chapter 2 documents that Digital Engineering has demonstrated value in aerospace and defense contexts. However, demonstrated value in one domain does not automatically transfer

to adoption in another. IT and Information Assurance professionals operate in different organizational contexts, face different constraints, and hold different professional identities than aerospace systems engineers. Whether these professionals recognize potential value in Digital Engineering capabilities for their work represents an open question that must be answered before implementation research becomes meaningful.

Furthermore, if professionals are unaware of Digital Engineering capabilities, no amount of demonstrated value will drive adoption because the capabilities will not enter consideration during tool selection, process design, or strategic planning. Establishing current awareness levels identifies whether education and communication initiatives represent necessary precursors to adoption efforts. If professionals are aware but do not perceive value, the theoretical premise that Digital Engineering addresses recognized needs within these domains requires reconsideration before investing in implementation research.

3.1.1.2 Why Not a Case Study or Implementation Pilot

This research considered and rejected alternative approaches for specific reasons. A case study examining Digital Engineering implementation within a specific organization would provide rich contextual data about practical implementation challenges and outcomes. However, case study findings would reflect the particular organizational context, culture, technical environment, and implementation approach of that organization. The findings would not establish whether the broader professional community recognizes value in Digital Engineering or possesses awareness of these capabilities. A successful case study might demonstrate technical feasibility without indicating whether adoption would occur beyond the studied organization.

An implementation pilot would face similar limitations while requiring access to organizational resources and authority to implement Digital Engineering tools and practices. Such a pilot would measure actual rather than perceived value, but would do so within a single organizational context that may not represent the broader population. Addition-

ally, implementation research presumes that the target professional community recognizes sufficient potential value to warrant the investment required for implementation. This presumption is precisely what the current research tests.

Survey research enables assessment across a broad population of practitioners, establishing baseline awareness and perceived value data that informs whether subsequent case study or implementation research would find receptive audiences. Survey methodology represents the appropriate starting point for investigating a nascent application domain where professional awareness and perceptions remain unknown.

3.1.1.3 Why Perceived Value Warrants Dissertation Research

Whether perceived value merits dissertation-level investigation reflects a particular view of research contribution. By addressing a documented gap, this research contributes to knowledge: the academic literature contains no investigation of whether IT and Information Assurance professionals perceive value in Digital Engineering capabilities. As Chapter 2 establishes, the theoretical framework posits that Digital Engineering offers solutions to documented problems in these domains. Testing whether practitioners recognize this potential value provides empirical grounding for the theoretical framework.

If research reveals that professionals recognize value in Digital Engineering capabilities, this finding validates the theoretical premise and establishes foundation for subsequent implementation research. If research reveals limited awareness or skepticism, this finding challenges the theoretical framework and identifies barriers that must be addressed before adoption can occur. Either outcome advances understanding and provides actionable direction for researchers and practitioners. The contribution lies not in advocating for Digital Engineering adoption but in establishing empirical evidence regarding professional perceptions that informs subsequent research and practice decisions.

3.1.2 Systems Engineering Approach to Research Design

To demonstrate strong rigor in the design, execution, analysis, and documentation of results, this research utilizes an approach that follows a systems engineering lifecycle. By applying systems engineering principles to this dissertation project, a strong degree of rigor and supporting artifacts lend structure and credibility to the dissertation process as a whole. The principal method of the dissertation effort is captured and tracked within a model to ensure traceability to decisions, citations, and artifacts—the same traceability that Digital Engineering brings to complex system development.

The survey model follows a structured lifecycle consisting of six phases:

3.1.2.1 Strategic Phase

Captures conceptual elements including hypothesis, capabilities, constraints, goals, vision, timeline, milestones, stakeholders, and drivers. This phase establishes the foundation for all subsequent research activities by clearly articulating what the research seeks to accomplish and why it matters.

3.1.2.2 Requirements Phase

Derives and analyzes strategic elements to create requirements for the dissertation and associated survey. Requirements follow ISO 15288:2023 standards: hierarchical in nature and structure, atomic in composition, bidirectional in traceability, individually measurable, and explicitly tracking relationships and interdependencies.

3.1.2.3 Architecture Phase

Establishes the high-level outline, structure, and guidance for the design and implementation phases of the dissertation. The survey architecture defines the overall structure of sections and question flow, ensuring logical progression from awareness through applica-

bility to perceived value.

3.1.2.4 Design Phase

Utilizes the architecture guidance and requirements to design the dissertation proposal and survey instrument, satisfying the architectural outline with complete traceability back to requirements and strategic elements.

3.1.2.5 Results Phase

Captures the survey data into the model for traceability along with results of analysis. Analysis methods and results are captured as elements within the model, enabling verification that findings address the original research questions.

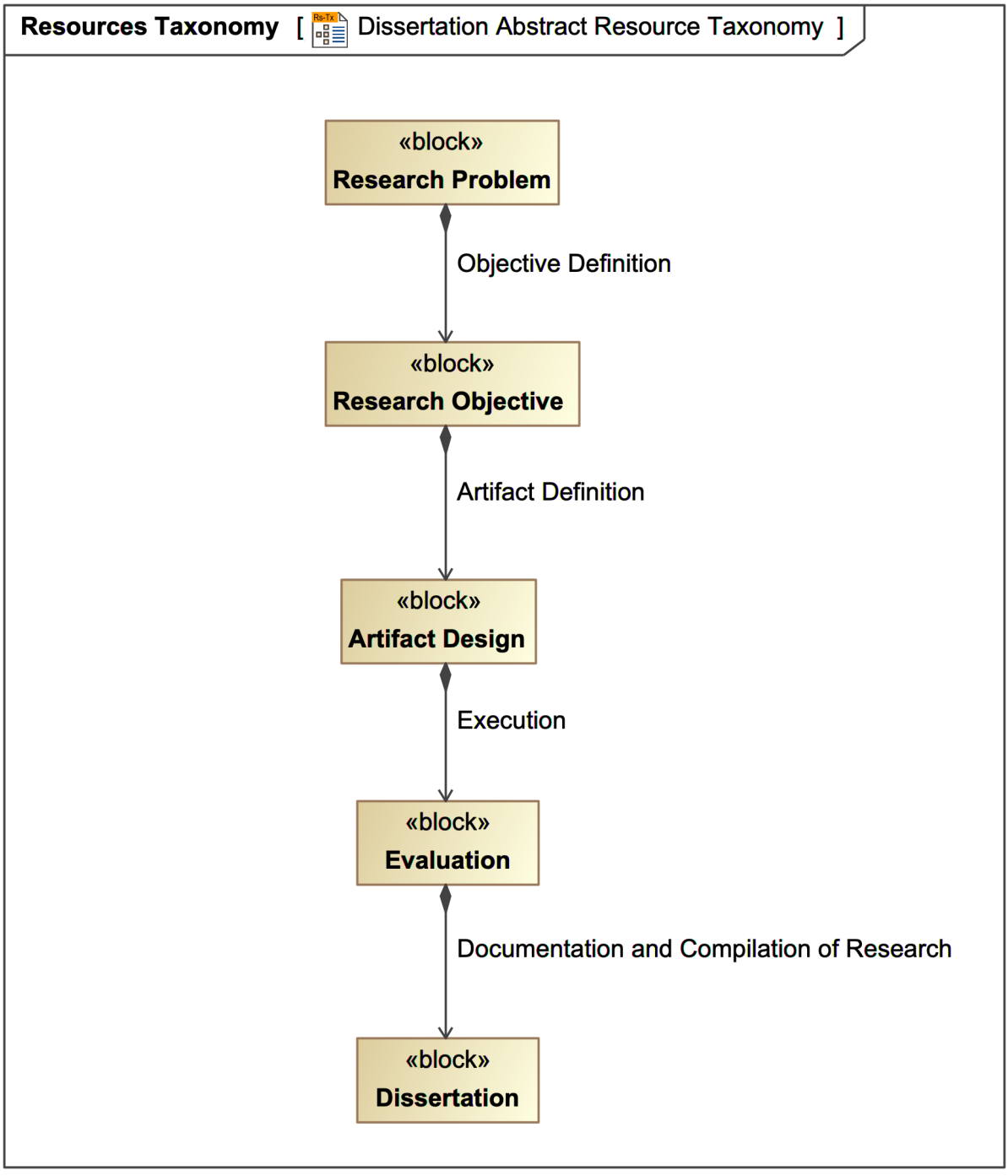
3.1.2.6 Report Phase

The model serves as a deliverable component of the dissertation that provides a rigorous source of artifacts, methodologies employed, traceability chains, and evidentiary support for the findings of the dissertation.

3.1.2.7 Alignment to Dissertation Design

Figure 3.1 provides a visual representation of the dissertation process utilizing an MBSE approach. This project has completed the design phase from a systems engineering lifecycle perspective, and the artifact design phase from a dissertation lifecycle perspective.

Figure 3.1: Dissertation Abstract Resource Taxonomy



3.1.3 Research Questions and Survey Alignment

The survey instrument was designed to directly address the three research questions:

3.1.3.1 Research Question 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?

3.1.3.2 Research Question 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?

3.1.3.3 Research Question 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?

Each survey section and question was mapped to these research questions to ensure comprehensive coverage of the research objectives while minimizing respondent burden through focused questioning. This mapping provides the traceability essential to demonstrating that the instrument measures what it purports to measure.

Figure 3.2 illustrates an MBSE representation of the Research Questions as requirement type elements. Selecting requirement type elements within the UAF allows survey questions to utilize “Satisfy” relationship. Authoritative traceability within the model enables programatic evaluation to validate the model.

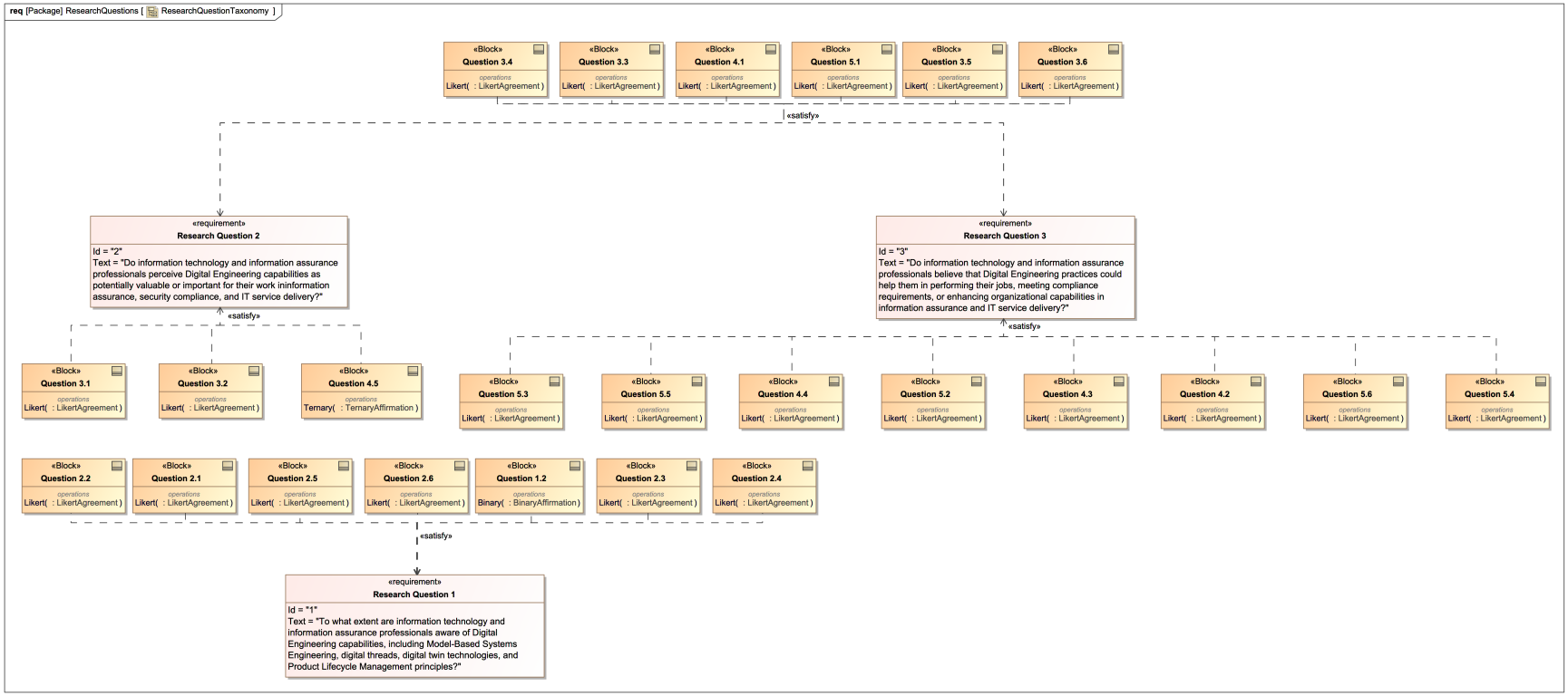


Figure 3.2: MBSE Instantiation of Research Questions

3.2 Survey Requirements Specification

Following the systems engineering approach, specific requirements were established for the survey instrument prior to design. These requirements ensure the survey meets research objectives while maintaining ethical standards and data quality. Requirements engineering precedes design—a principle as valid in research methodology as in systems development.

3.2.1 Anonymity and Privacy Requirements

The following requirements govern anonymity and privacy protection:

- The survey shall be anonymous, collecting no personally identifiable information during the survey process.
- The survey shall not collect age, sex, gender, race, creed, gender identity, sexual orientation, income, nationality, or other non-relevant personal information.
- The survey shall be protected with appropriate security controls to ensure the confidentiality, integrity, and availability of collected data.
- The survey raw data shall not be sold or used for any purpose other than the dissertation research.

3.2.2 Instrument Design Requirements

The following requirements govern survey instrument design:

- The survey shall utilize a Likert Scale for material research questions to enable quantitative analysis.
- The survey shall include applicable notices required by the University Institutional Review Board.

- The survey should collect demographic information to identify the participant's professional field of study or practice.
- The survey should collect demographic information about temporal experience level within the participant's field.

3.2.3 Content Requirements

Survey content is structured to assess the awareness, applicability, and perceived value that participants hold toward Digital Engineering and its component disciplines. Beginning at the enterprise level, the survey then examines the four pillars: Model-Based Systems Engineering, the Digital Thread, Digital Twin, and Product Lifecycle Management. Consistent question flow across this structure enables analysis of how each discipline is perceived in relation to Digital Engineering as a unified approach.

Value assessment questions in Sections 3 through 5 employ positively framed capability statements (e.g., "Digital Engineering could deliver meaningful value" or "could reduce development cycle time"). Deliberate design decisions informed by the research objectives and target population characteristics underlie this framing. Because the research questions ask whether professionals perceive value in Digital Engineering capabilities, positively framed statements directly measure this construct by presenting capabilities and assessing agreement. An instrument measuring perceived value necessarily presents value propositions for evaluation. Negatively framed items (e.g., "Digital Engineering would not improve security posture") would introduce cognitive complexity through double negatives when combined with disagreement responses, a confound well documented in survey methodology literature that disproportionately affects respondents unfamiliar with the subject matter.

To mitigate the acquiescence bias risk inherent in consistently framed questions, several instrument-level safeguards are employed. A neutral midpoint ("Neither agree nor disagree") provides a non-affirmative response option for respondents who are genuinely

uncertain or indifferent. Additionally, the binary and ternary investment willingness questions (Questions 4.5 and 5.7) offer explicit "No" and "Unsure" options that capture skepticism and uncertainty without requiring disagreement with a positively framed statement. Section 1 familiarity self-assessment provides an independent baseline against which value perception scores can be interpreted; respondents reporting low familiarity who nonetheless indicate high agreement with value statements can be identified and examined as a potential indicator of acquiescence rather than genuine perception. During analysis, response pattern analysis shall examine whether any respondents demonstrate uniform agreement across all items, a pattern suggestive of satisficing or acquiescence rather than considered evaluation.

3.3 Target Population and Sampling

3.3.1 Target Population

Professionals actively working in information technology and information assurance roles within organizations that manage information systems constitute the target population for this study. Encompassing individuals involved in IT service delivery, infrastructure management, service operations, information assurance, security operations, compliance management, and security architecture, the population spans organizational types including private sector enterprises, government agencies, educational institutions, and nonprofit organizations.

The dual focus upon information technology and information assurance professionals recognizes that Digital Engineering capabilities may offer distinct value propositions for these related but different professional communities. IT professionals primarily concerned with service delivery and operational efficiency may perceive value in Digital Engineering practices differently than information assurance professionals focused upon threat mitigation, compliance verification, and security control implementation. Understanding both

perspectives is necessary for thorough assessment.

3.3.2 Sampling Strategy

This study employs non-probability convenience sampling to recruit participants through professional networks, industry associations, and online professional communities. While probability sampling would provide stronger generalizability, the difficulty of establishing a sampling frame for all IT and information assurance professionals renders probability sampling impractical for this research. Convenience sampling enables efficient access to qualified respondents while maintaining focus upon professionals with relevant experience and expertise.

To enhance the representativeness of the convenience sample, recruitment efforts target multiple channels including professional organizations such as ISACA, $(ISC)^2$, and ITIL professional communities; LinkedIn professional groups focused upon IT service management and information assurance; industry conferences and professional development events; and direct outreach to IT and security departments within organizations across multiple sectors. This multi-channel approach mitigates the limitations inherent in convenience sampling.

3.3.3 Sample Size Determination

The required sample size was calculated to achieve a maximum margin of error of five percent at the 95% confidence level. For survey research targeting a large population where the population size exceeds 100,000 individuals, the sample size formula for estimating a proportion is:

$$n = \frac{Z^2 \times p \times (1 - p)}{E^2} \tag{3.1}$$

Where:

- n = required sample size
- Z = Z-score for desired confidence level (1.96 for 95% confidence)
- p = estimated population proportion (0.5 for maximum variability)
- E = desired margin of error (0.05 for 5%)

Substituting these values:

$$n = \frac{1.96^2 \times 0.5 \times 0.5}{0.05^2} = \frac{3.8416 \times 0.25}{0.0025} = \frac{0.9604}{0.0025} = 384.16 \tag{3.2}$$

Therefore, a minimum of 385 completed survey responses is required to achieve the target margin of error. This calculation assumes maximum variability in responses (p = 0.5), which provides the most conservative sample size estimate. If actual response distributions demonstrate less variability, the effective margin of error will be smaller than five percent.

To account for potential incomplete responses and to ensure adequate representation across professional subgroups—IT professionals versus security professionals, varying experience levels—the target sample size for data collection is set at 450 completed surveys. This target represents approximately seventeen percent above the minimum requirement, aligning with survey research best practices recommending fifteen to twenty percent oversampling to accommodate anticipated attrition [151]. Research on online survey completion rates indicates that professional surveys typically experience ten to fifteen percent incomplete response rates due to survey abandonment, partial completion, or data quality concerns requiring exclusion [152]. The 450-response target provides sufficient buffer to ensure the minimum 385 usable responses while enabling meaningful subgroup analyses with adequate statistical power. Specifically, if the sample divides evenly between IT and security professionals, each subgroup would include approximately 190-225 respondents, providing margins of error between six and seven percent for subgroup-specific analyses.

3.4 Survey Instrument Design

3.4.1 Instrument Overview

Consisting of 27 questions organized into six thematic sections, the survey instrument was designed to systematically address the research questions while maintaining reasonable completion time. An estimated completion time of approximately ten minutes was established through consideration of question complexity and respondent fatigue factors, balancing comprehensive data collection against respondent engagement and completion rates. Brevity serves validity: a shorter survey that respondents complete thoughtfully yields better data than a longer survey that respondents abandon or rush through.

The six sections are structured as follows:

1. Section 1: Awareness and Familiarity with Digital Engineering (2 questions)
2. Section 2: Understanding of Digital Engineering Capabilities (6 questions)
3. Section 3: Applicability of Digital Engineering (6 questions)
4. Section 4: Value Assessment for Information Technology (5 questions)
5. Section 5: Value Assessment for Information Assurance and Cybersecurity (7 questions)
6. Section 6: Interest and Demographic Information (4 questions)

3.4.2 Question Format and Scale Selection

Two primary question formats are employed: five-point Likert-type scales and binary (yes/no) response options. Selection of these formats was guided by psychometric research establishing their validity and reliability for measuring attitudes, perceptions, and self-reported behaviors.

3.4.2.1 Likert Scale Justification

The five-point Likert scale format was selected for questions measuring awareness levels, agreement with capability statements, and perceptions of value. Likert scales have been extensively validated for measuring attitudes and perceptions in social science research since their introduction by Rensis Likert in 1932. The five-point format specifically was chosen based upon research demonstrating that five to seven response options provide optimal discrimination between respondent positions while remaining cognitively manageable for respondents. More options add complexity without proportionate gain in discriminatory power.

The analytical treatment of Likert scale data warrants explicit methodological comment. A longstanding debate in psychometric and social science research concerns whether Likert scale responses constitute ordinal data (where distances between scale points are not necessarily equal) or may be treated as interval data (where parametric statistical methods such as means and standard deviations are appropriate). Jamieson [153] argues that Likert data are strictly ordinal and that parametric analyses may produce misleading results. Norman [154], drawing upon extensive simulation research, demonstrates that parametric methods are sufficiently robust to yield valid results with Likert data even when distributional assumptions are violated. Subsequent research by Sullivan and Artino [155] and de Winter and Dodou [156] supports Norman's position, finding that parametric tests applied to five-point Likert data produce conclusions consistent with non-parametric alternatives across a wide range of distributional conditions.

This research follows the analytical convention adopted by the majority of technology acceptance and survey research: parametric descriptive statistics (means, standard deviations) are reported for Likert items and composite scores to enable comparison with the broader literature, while non-parametric alternatives are employed for inferential testing when distributional assumptions are not met. Specifically, Shapiro-Wilk tests and visual inspection of distributions determine whether parametric tests (t-tests, ANOVA)

or non-parametric alternatives (Mann-Whitney U, Kruskal-Wallis) are applied for group comparisons. Medians and interquartile ranges are reported alongside means and standard deviations for individual Likert items, providing readers with both parametric and ordinal summaries. This dual-reporting approach ensures transparency and enables readers who hold either position in the ordinal-interval debate to evaluate the findings against their preferred analytical framework.

Consistent use of Likert scales across sections provides an intuitive response method for participants and enables direct comparison of responses across different constructs. Two distinct anchor sets are employed depending upon the construct being measured:

3.4.2.1.1 Familiarity Scale (Section 1, Question 1.1)

1. Not at all familiar
2. Slightly familiar
3. Moderately familiar
4. Very familiar
5. Extremely familiar

3.4.2.1.2 Agreement Scale (Sections 2-5)

1. Strongly disagree
2. Disagree
3. Neither agree nor disagree
4. Agree
5. Strongly agree

Following established conventions in technology acceptance research, including the Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) frameworks, the agreement scale has demonstrated validity for measuring perceptions of technology value and usefulness across diverse populations and contexts. Including a neutral midpoint ("Neither agree nor disagree") enables respondents to indicate genuine uncertainty rather than forcing artificial choices, which research suggests improves response validity. Figure 3.3 demonstrates the instantiation of familiarity and agreement response scales within the model of the dissertation survey.

3.4.2.2 Binary and Ternary Question Justification

Binary yes/no, and ternary yes/no/unsure questions are employed for factual questions about prior exposure (Section 1, Question 1.2), interest in further learning (Section 6, Questions 6.1-6.2), and investment willingness (Sections 4-5, Questions 4.5 and 5.7). Binary/ternary formats are appropriate for these questions because they seek to classify respondents into discrete categories rather than measure degrees of agreement or perception intensity. The simplicity of binary/ternary responses also reduces cognitive load for straightforward factual questions where graduated responses would add complexity without meaningful information gain. Figure 3.3 provides a visualization of the enumeration elements of the binary and ternary responses.

3.4.2.3 Categorical Questions

Section 6 includes categorical questions capturing demographic information about professional field of practice and years of experience. Following the demographic information requirements, these questions capture only sector of work and temporal experience level without collecting personally identifiable information. The experience level categories are structured to capture early career, mid-career, and late career stages:

- 1-5 Years of experience (Early Career)

- 6-10 Years of experience (Mid Career - Early)
- 11-15 Years of experience (Mid Career - Late)
- 16+ Years of experience (Late Career)

These categories enable analysis of response patterns across professional subgroups and experience levels, supporting investigation of whether awareness and perceptions vary systematically by professional background. Such variation would carry significant implications for professional development and adoption strategies.

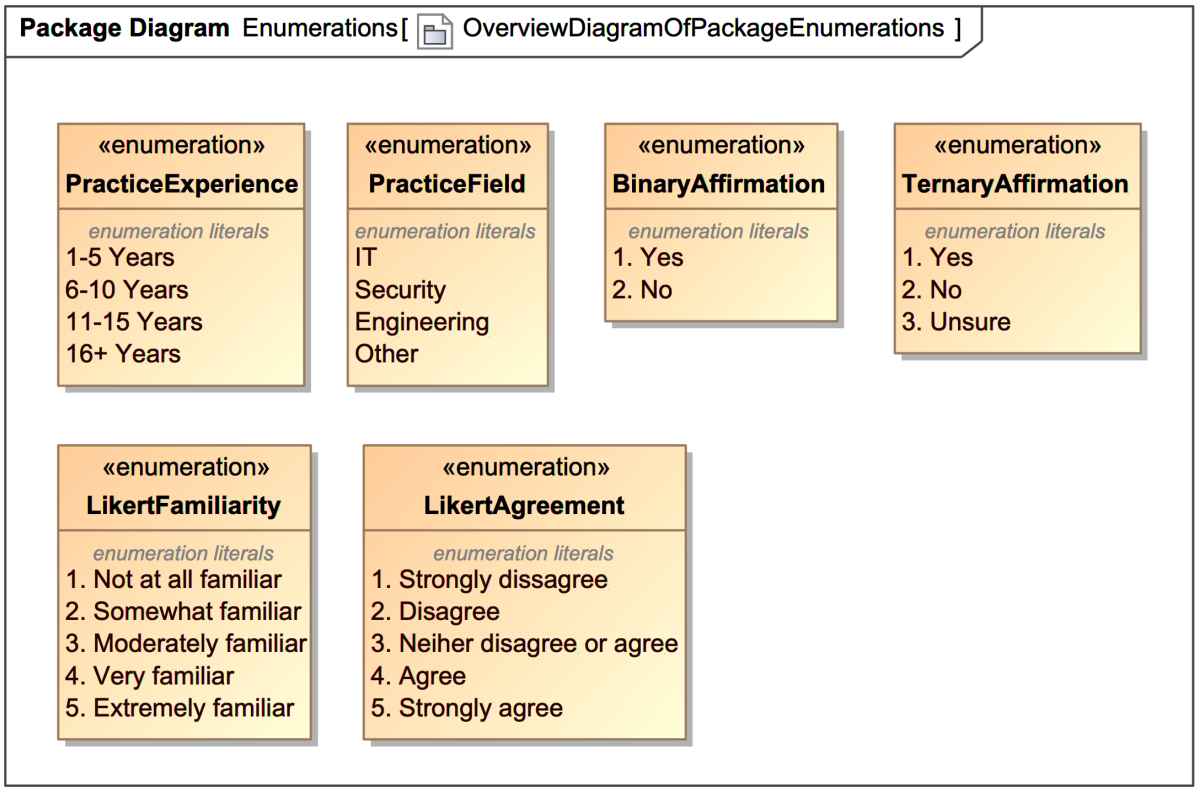


Figure 3.3: Survey Question Enumeration

3.5 Survey Section Structure and Research Question Mapping

Detailing how each survey section addresses the research questions, this section provides explicit traceability between survey content and research objectives. Every question serves a defined purpose, and the mapping ensures that the research questions receive comprehensive coverage.

3.5.1 Section 1: Awareness and Familiarity with Digital Engineering

Section 1 contains two questions directly addressing Research Question 1 regarding professional awareness of Digital Engineering capabilities. Figure 3.5 provides an MBSE based visualization as a block element.

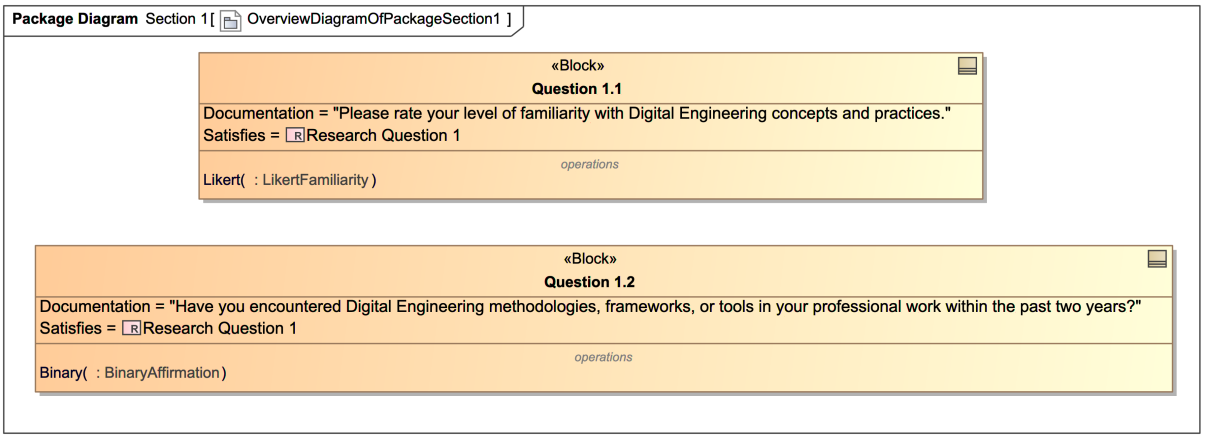


Figure 3.4: Survey Questions Section 1 Detailed Properties Taxonomy

3.5.1.1 Question 1.1

This question utilizes a five-point familiarity scale to measure self-reported awareness levels: “Please rate your level of familiarity with Digital Engineering concepts and practices.” This question provides a direct, self-assessed measure of overall Digital Engineering

awareness—the baseline from which all subsequent analysis proceeds.

3.5.1.2 Question 1.2

This question employs a binary format to determine recent professional exposure: "Have you encountered Digital Engineering methodologies, frameworks, or tools in your professional work within the past two years?" This question distinguishes between theoretical awareness and practical professional experience, recognizing that knowing about Digital Engineering differs categorically from having encountered it in practice.

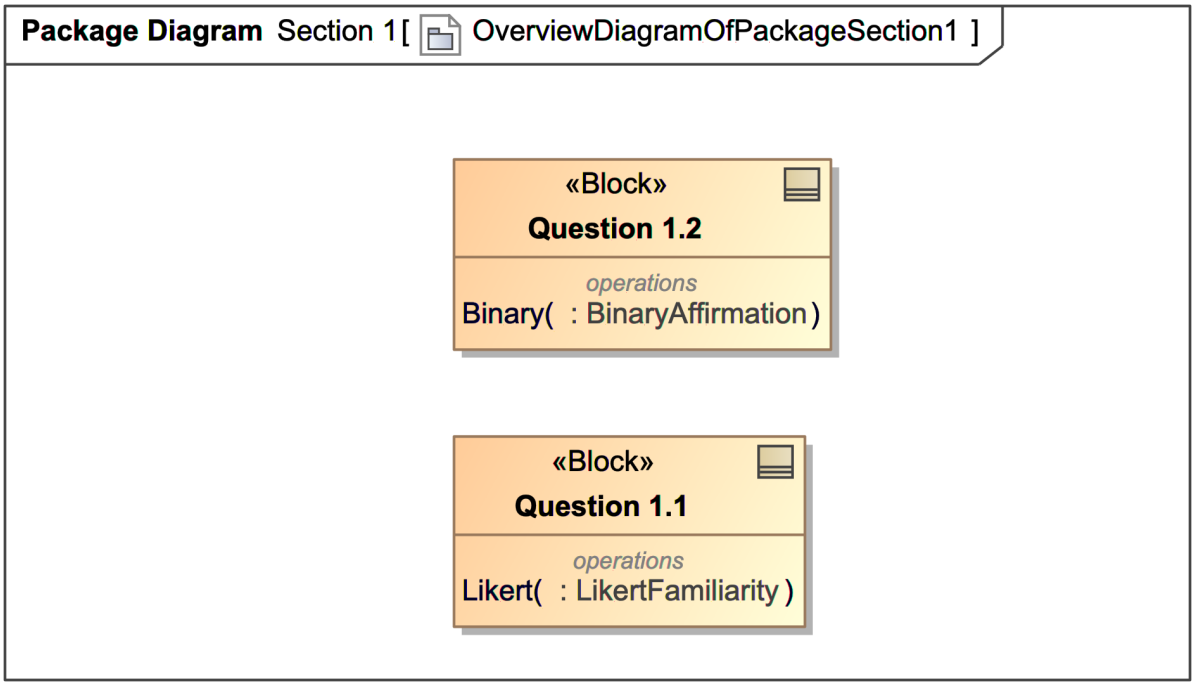


Figure 3.5: Section One Survey Question Elements Package Diagram

3.5.1.3 Mapping to Research Question 1

These questions directly measure the extent of professional awareness, providing quantifiable data on familiarity levels and recent professional exposure to Digital Engineering concepts.

3.5.2 Section 2: Understanding of Digital Engineering Capabilities

Section 2 contains six Likert-scale questions assessing respondent understanding of specific Digital Engineering capabilities. Figure 3.6 visualizes each research question as represented in the model. The questions of Section 2 probe awareness of the four Digital Engineering pillars in the context of IT and information assurance applications:

3.5.2.1 Question 2.1

This question addresses Model-Based Systems Engineering: "Digital Engineering includes model-based systems engineering approaches that can improve development processes."

3.5.2.2 Question 2.2

This question addresses Digital Twin for IT: "Digital Engineering can enable digital twin development and virtual prototyping for information technology systems."

3.5.2.3 Question 2.3

This question addresses the Digital Thread and data-driven practices: "Digital Engineering supports continuous integration and data-driven decision-making in technology development."

3.5.2.4 Question 2.4

This question addresses Digital Twin for security: "Digital Engineering enables digital twin technology that can simulate security scenarios and test defensive measures without impacting production systems."

3.5.2.5 Question 2.5

This question addresses security validation through the Digital Thread: "Digital Engineering supports continuous security validation and data-driven threat analysis throughout the development lifecycle."

3.5.2.6 Question 2.6

This question addresses compliance automation: "Digital Engineering can improve security control implementation through automated compliance checking and verification."

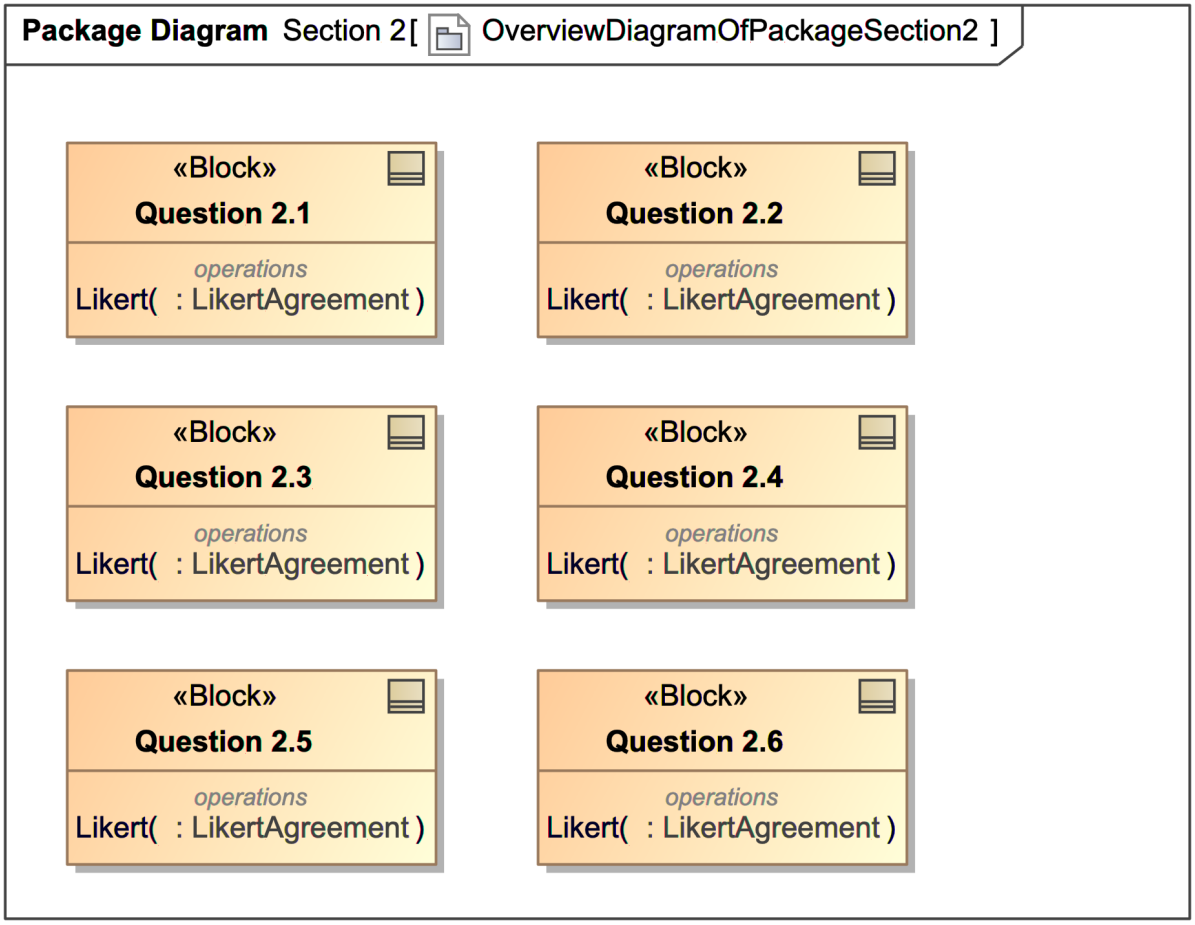


Figure 3.6: Section Two Survey Question Elements Package Diagram

3.5.2.7 Mapping to Research Question 1

This section extends Research Question 1 by measuring not only general awareness but comprehension of specific Digital Engineering pillars—MBSE, Digital Twin, the Digital Thread, and PLM—and their applications to IT and information assurance contexts. A methodological distinction warrants clarification: Section 2 questions employ agreement scales rather than direct awareness measures. Agreement with a capability statement (e.g., "Digital Engineering includes model-based systems engineering approaches that can improve development processes") captures a construct more precisely characterized as informed comprehension—whether respondents recognize and affirm the described capability relationship—rather than simple awareness of terminology. This design choice reflects the research objective of assessing whether professionals understand what Digital Engineering capabilities entail, not merely whether they have heard the term. Section 1 captures the latter construct directly through familiarity self-assessment; Section 2 probes deeper by testing whether familiarity corresponds to substantive understanding of capability descriptions. Taken together, Sections 1 and 2 provide a layered assessment of Research Question 1 that distinguishes surface-level awareness from functional comprehension.

3.5.3 Section 3: Applicability of Digital Engineering

Section 3 contains six Likert-scale questions examining perceptions of Digital Engineering applicability to information technology and information assurance domains. This section bridges awareness assessment and value perception, probing whether respondents see relevance to their professional contexts. Instantiation of section 3 survey questions within the model are visualized in Figure 3.7.

3.5.3.1 Question 3.1

This question assesses IT sector relevance: "Digital Engineering methodologies have relevant applications within the information technology sector."

3.5.3.2 Question 3.2

This question assesses Information Assurance relevance: "Digital Engineering methodologies have relevant applications for addressing information assurance challenges."

3.5.3.3 Question 3.3

This question assesses Digital Twin organizational value: "The ability to utilize digital twins to test changes against accurate replicas of production environments would provide value to my organization."

3.5.3.4 Question 3.4

This question assesses MBSE organizational value: "The use of digital models to map and document an organization's environment and configurations would provide value to my organization."

3.5.3.5 Question 3.5

This question assesses PLM organizational value: "The use of digital lifecycle management to meet compliance and service delivery requirements would provide value to my organization."

3.5.3.6 Question 3.6

This question assesses compliance applicability: "My organization faces regulatory or compliance requirements that could benefit from Digital Engineering approaches."

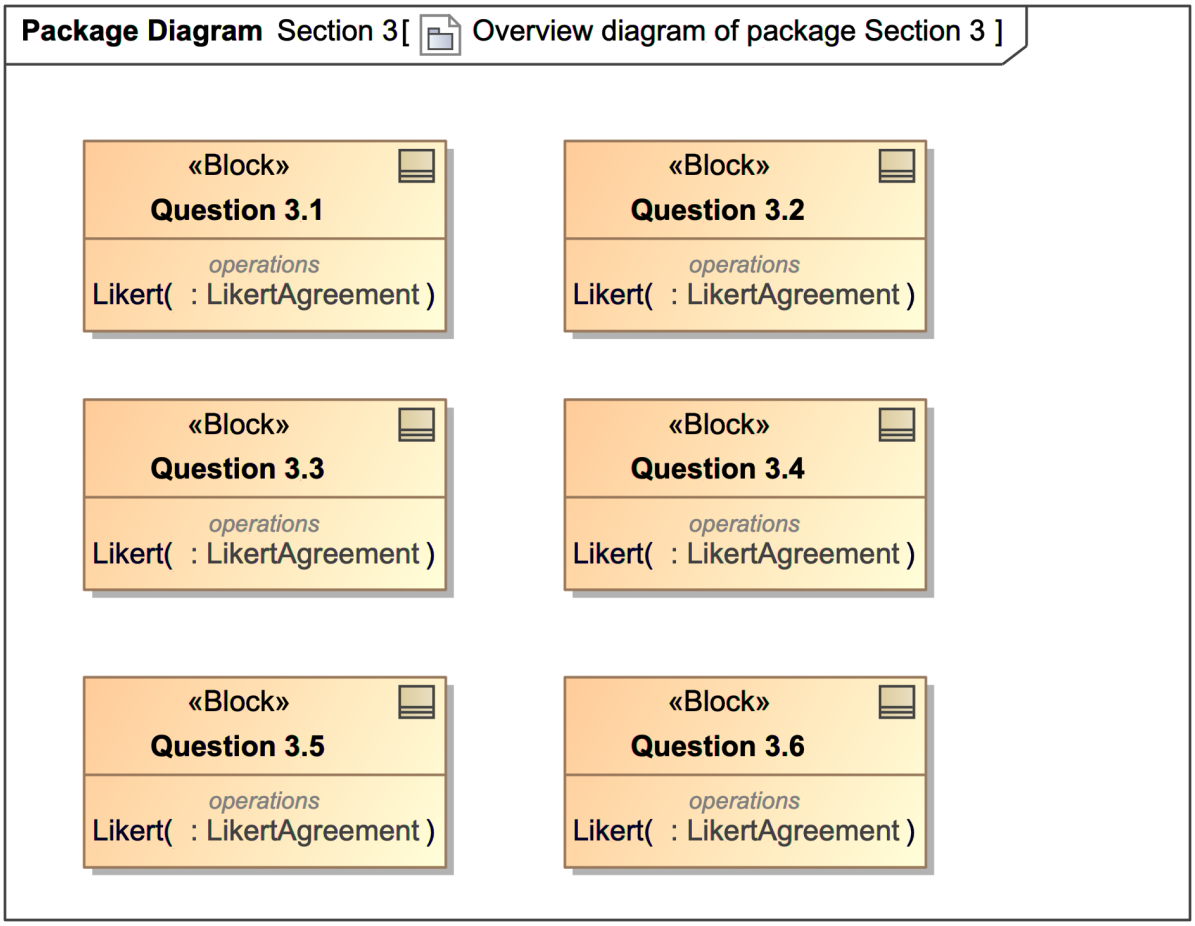


Figure 3.7: Section Three Survey Question Elements Package Diagram

3.5.3.7 Mapping to Research Questions 2 and 3

This section addresses whether respondents perceive Digital Engineering as applicable to their professional domains and whether they identify potential organizational value in specific capabilities.

3.5.4 Section 4: Value Assessment for Information Technology

Section 4 contains five questions assessing perceived value of Digital Engineering for IT operations specifically, and are visualized in Figure 3.8

3.5.4.1 Question 4.1

This question measures overall IT value: "Digital Engineering could deliver meaningful value to my organization's information technology processes."

3.5.4.2 Question 4.2

This question measures cycle time benefit: "Digital Engineering could reduce development cycle time in my organization."

3.5.4.3 Question 4.3

This question measures quality benefit: "Digital Engineering could improve product quality and reduce defects in my organization."

3.5.4.4 Question 4.4

This question measures collaboration benefit: "Digital Engineering could improve collaboration effectiveness across development teams in my organization."

3.5.4.5 Question 4.5

This question measures investment willingness: "My organization would be willing to invest in Digital Engineering capabilities if clear return on investment could be demonstrated." (Yes/No/Unsure)

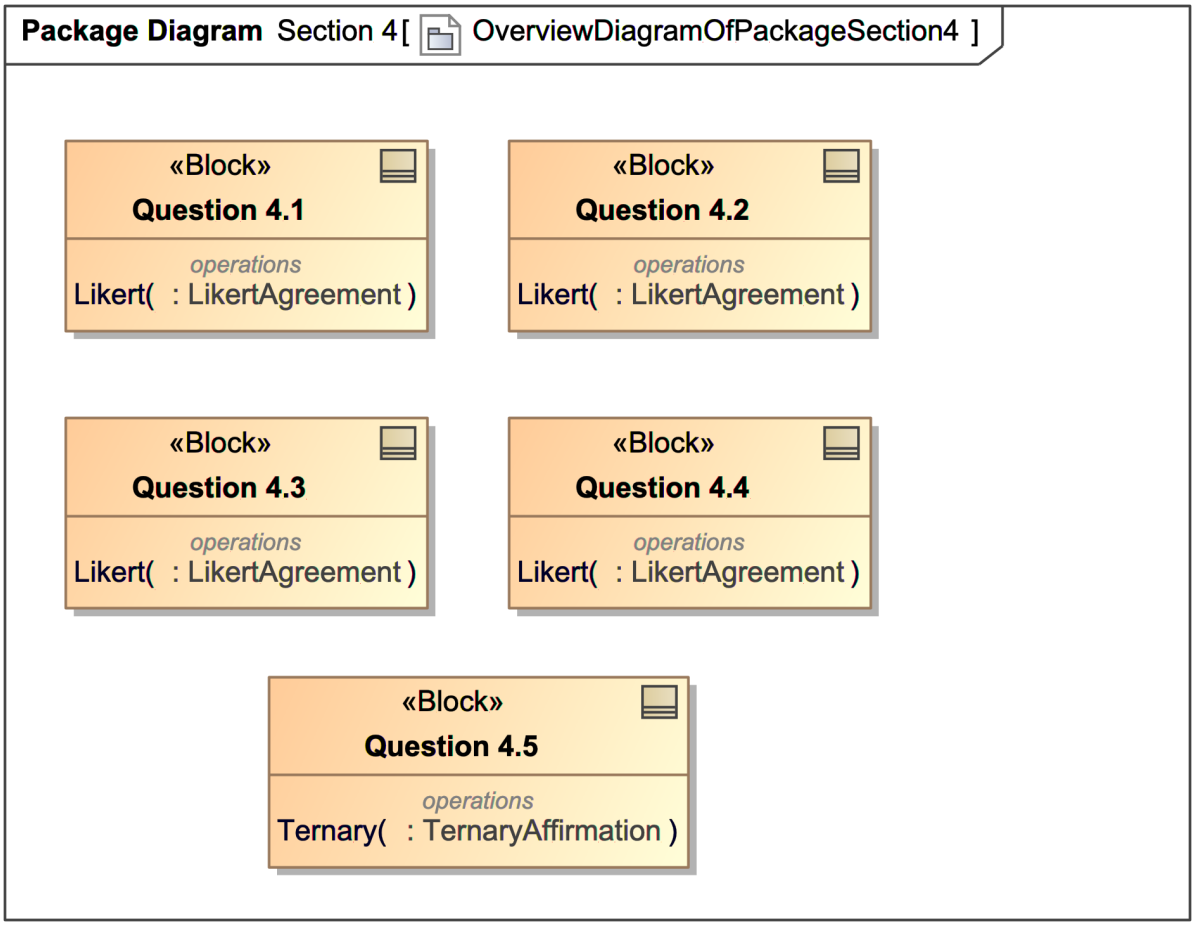


Figure 3.8: Section Four Survey Question Elements Package Diagram

3.5.4.6 Mapping to Research Questions 2 and 3

This section directly addresses whether IT professionals perceive value in Digital Engineering and believe these practices could enhance their organizational capabilities and job performance.

3.5.5 Section 5: Value Assessment for Information Assurance and Cybersecurity

Section 5 contains seven questions assessing perceived value of Digital Engineering for information assurance and cybersecurity operations as displayed in Figure 3.9.

3.5.5.1 Question 5.1

This question measures overall security value: "Digital Engineering could deliver meaningful value to my organization's information assurance and cybersecurity operations."

3.5.5.2 Question 5.2

This question measures vulnerability management benefit: "Digital Engineering could reduce the time required to identify and remediate security vulnerabilities in my organization."

3.5.5.3 Question 5.3

This question measures security posture benefit: "Digital Engineering could improve security posture and reduce successful cyber incidents in my organization."

3.5.5.4 Question 5.4

This question measures threat modeling benefit: "Digital Engineering could enhance threat modeling and risk assessment capabilities in my organization."

3.5.5.5 Question 5.5

This question measures cross-team collaboration benefit: "Digital Engineering could improve collaboration between security teams, development teams, and operations teams in my organization."

3.5.5.6 Question 5.6

This question measures compliance benefit: "Digital Engineering could help my organization achieve better compliance with security frameworks and regulatory requirements."

3.5.5.7 Question 5.7

This question measures security investment willingness: "My organization would be willing to invest in Digital Engineering capabilities for cybersecurity purposes if clear return on investment could be demonstrated." (Yes/No/Unsure)

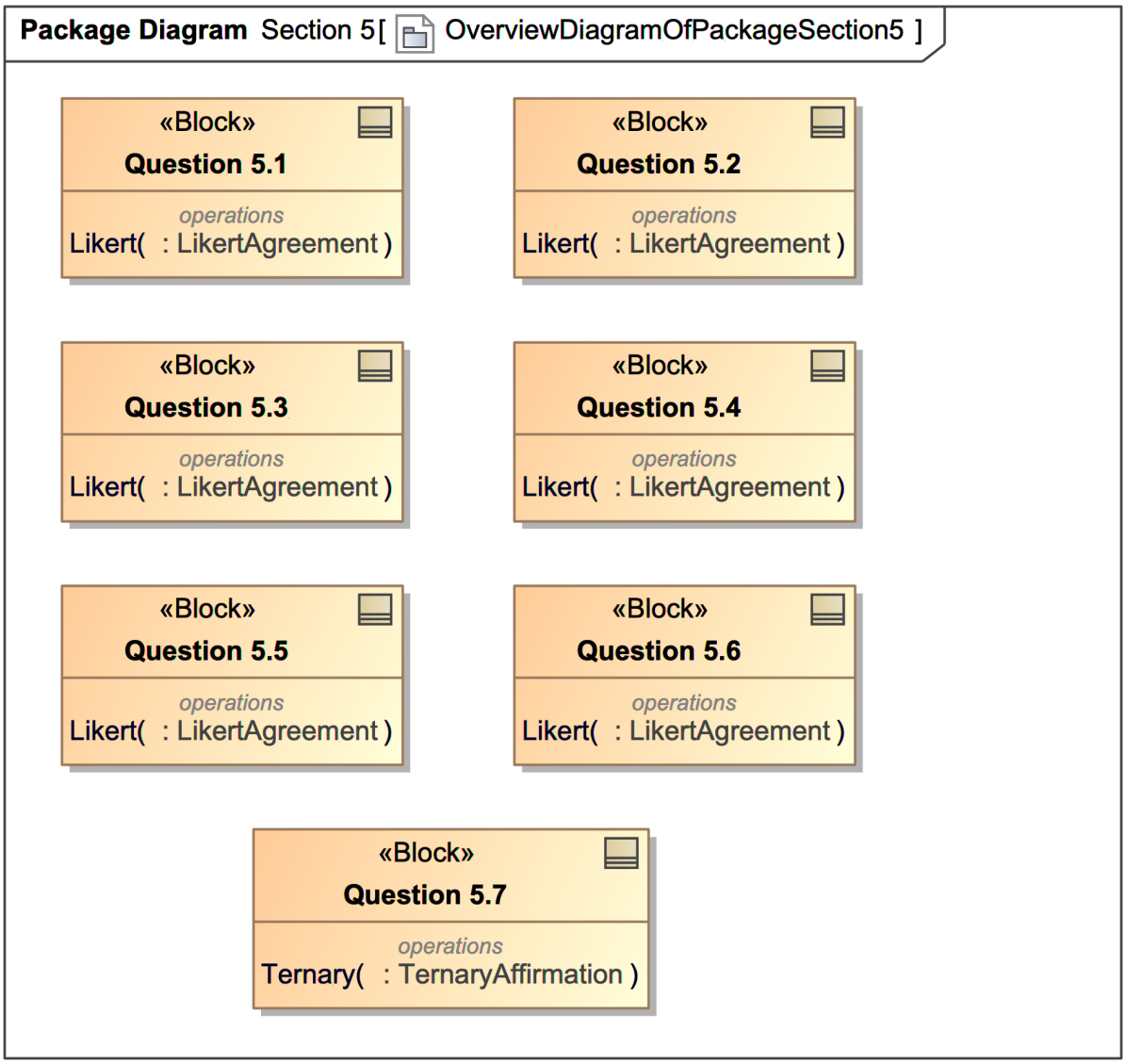


Figure 3.9: Section Five Survey Question Elements Package Diagram

3.5.5.8 Mapping to Research Questions 2 and 3

This section directly addresses whether information assurance professionals perceive value in Digital Engineering for their specific domain and believe these practices could help them meet compliance requirements and enhance security capabilities.

3.5.6 Section 6: Interest and Demographic Information

Section 6 contains four questions capturing respondent interest in Digital Engineering learning opportunities and demographic characteristics. Figure 3.10 visualizes section 6 survey questions.

3.5.6.1 Question 6.1

This question measures learning interest: "Would you be interested in learning more about Digital Engineering applications for information assurance and cybersecurity in your industry?"

3.5.6.2 Question 6.2

This question measures recommendation likelihood: "Would you recommend that your organization explore Digital Engineering adoption for improving security operations?"

3.5.6.3 Question 6.3

Capturing professional field, this question asks: "Please indicate your field of practice." (Information Technology / Security / Engineering / Other). Using "Security" rather than "Information Assurance" as a response category reflects a practical design choice: working professionals identify their field using varied terminology including cybersecurity, information security, and information assurance. As a broader term, "Security" captures respondents across these self-identification preferences without excluding professionals

who may not associate their work with the specific term "information assurance" despite performing roles that fall within that discipline as defined in Chapter 1.

3.5.6.4 Question 6.4

This question captures experience level: "Please indicate your level of experience in your field of practice." (1-5 Years / 6-10 Years / 11-15 Years / 16+ Years)

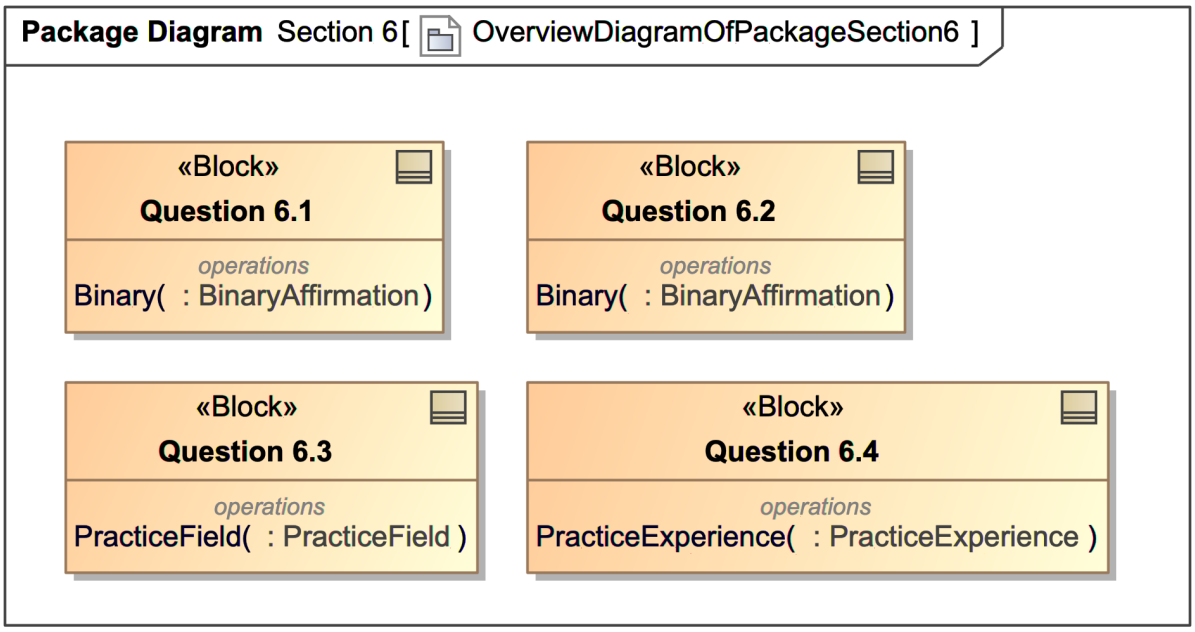


Figure 3.10: Section Six Survey Question Elements Package Diagram

3.5.6.5 Mapping to Research Questions

While not directly measuring awareness or perceived value, demographic data enables investigation of whether awareness and perceptions vary by professional field or experience level, providing insights for targeted future research and professional development initiatives.

3.5.7 Traceability of Survey Questions

Figure 3.11 provides a comprehensive diagram which shows authoritative traceability of survey question elements to the research questions. Use of relationship traceability diagrams enables validation with programatic diagrams.

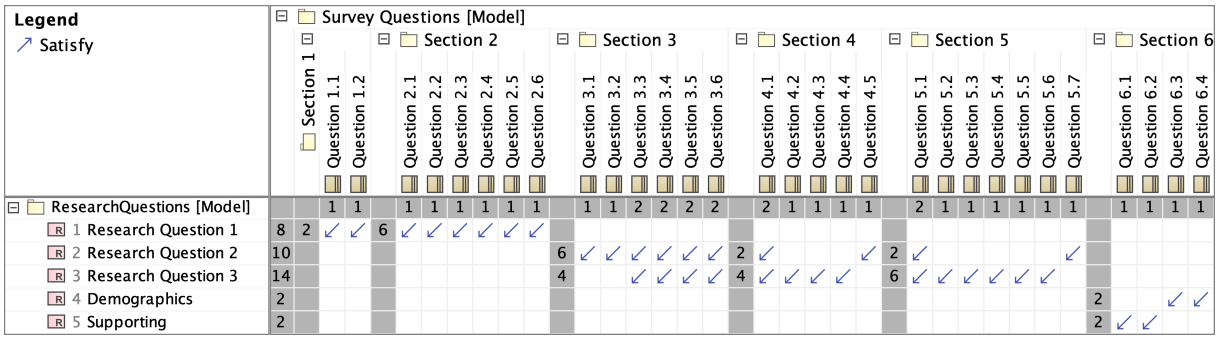


Figure 3.11: Research Question Traceability

3.6 Data Collection Procedures

3.6.1 Survey Platform and Administration

The survey shall be administered electronically using an established survey platform that supports anonymous response collection, secure data storage, and compliance with research ethics requirements. Electronic administration enables efficient access to geographically distributed respondents while ensuring consistent question presentation and response capture across all participants.

3.6.2 Data Protection Plan

In accordance with survey requirements, the survey data shall be protected with appropriate security controls to ensure the confidentiality, integrity, and availability of collected data. The data protection plan includes:

- Password protection and multifactor authentication for access to survey administration and data
- Encryption at rest for stored survey responses
- Encryption in transit for data transmission between respondents and the survey platform
- No collection of IP addresses or other metadata that could potentially identify respondents
- Secure storage in compliance with university data governance requirements

3.6.3 Informed Consent

Beginning with a comprehensive participation notice, the survey explains the research purpose, what participation involves, confidentiality protections, voluntary nature of participation, and contact information for questions or concerns. Specifically, the notice states:

- The survey is conducted as part of a doctoral research project at Dakota State University
- Participation is completely anonymous with no personally identifiable information collected
- Risks of participation are minimal and similar to those encountered in normal daily internet activity
- Participation is entirely voluntary with the right to withdraw at any time before submission
- Respondents must be 18 years or older to participate

- No compensation or incentive is offered for participation
- Completion and submission of the survey constitutes informed consent

3.6.4 Recruitment and Distribution

Survey distribution shall occur through multiple channels to maximize reach and diversity of the respondent pool. Recruitment messages shall clearly describe the target population (IT and information assurance professionals), estimated completion time (approximately ten minutes), and research purpose. Distribution channels include direct outreach to professional networks, posting in relevant online professional communities, distribution through professional association newsletters and communication channels, and sharing through academic and industry conference participants.

3.7 Data Analysis Plan

3.7.1 Data Preparation and Cleaning

Prior to analysis, survey responses shall be reviewed for completeness and data quality. Responses with substantial missing data (more than 20% of questions unanswered) shall be excluded from analysis. Remaining missing values shall be handled through listwise deletion for specific analyses where required variables are missing. Data quality precedes data analysis: conclusions drawn from flawed data remain flawed regardless of analytical sophistication.

3.7.2 Descriptive Statistical Analysis

Descriptive statistics shall be calculated for all survey questions to characterize the distribution of responses. For Likert-scale questions, analysis shall include frequency distributions, mean scores, median scores, and standard deviations. For binary and categorical

questions, analysis shall include frequency counts and percentages within each response category.

3.7.2.1 Research Question 1 Analysis

Analysis addressing Research Question 1 shall focus upon Sections 1 and 2 responses to characterize professional awareness of Digital Engineering capabilities. Key metrics include:

- Distribution of familiarity ratings from Question 1.1, with percentage of respondents at each familiarity level
- Percentage of respondents reporting professional exposure to Digital Engineering within the past two years (Question 1.2)
- Mean agreement scores and standard deviations for understanding of specific capabilities (Questions 2.1-2.6)
- Percentage of respondents indicating agreement (score ≥ 4) with each capability statement

Results shall be reported with 95% confidence intervals to indicate the precision of population estimates. For the target sample size of 385 respondents, the margin of error for reported proportions shall not exceed 5%.

3.7.2.2 Research Question 2 Analysis

Analysis addressing Research Question 2 shall focus upon Sections 3, 4, and 5 responses measuring perceived value of Digital Engineering capabilities. Key metrics include:

- Mean agreement scores and response distributions for applicability questions (Questions 3.1-3.6)

- Mean agreement scores and response distributions for IT value assessment questions (Questions 4.1-4.4)
- Mean agreement scores and response distributions for cybersecurity value assessment questions (Questions 5.1-5.6)
- Percentage of respondents indicating organizational investment willingness (Questions 4.5 and 5.7)

Responses indicating agreement (score = 4) or strong agreement (score = 5) with value statements shall be interpreted as evidence that professionals perceive potential value in Digital Engineering capabilities.

3.7.2.3 Research Question 3 Analysis

Analysis addressing Research Question 3 shall focus upon questions specifically addressing job performance, compliance requirements, and organizational capability enhancement. Key questions include:

- Question 3.5: Digital lifecycle management for compliance and service delivery
- Question 3.6: Regulatory or compliance requirements that could benefit from Digital Engineering
- Question 4.1: Meaningful value to IT processes
- Questions 4.2-4.4: Specific IT operational benefits (cycle time, quality, collaboration)
- Question 5.1: Meaningful value to cybersecurity operations
- Questions 5.2-5.6: Specific security operational benefits (vulnerability remediation, security posture, threat modeling, collaboration, compliance)

The percentage of respondents indicating agreement with these statements shall provide direct evidence regarding whether professionals believe Digital Engineering could help them in their work.

3.7.3 Comparative Analysis

Comparative analyses shall examine whether awareness levels and value perceptions differ significantly between professional subgroups and experience levels. Such differences would carry significant implications for adoption strategies and professional development initiatives.

3.7.3.1 Professional Field Comparison

Independent samples t-tests or Mann-Whitney U tests shall compare responses between IT professionals and security professionals (based upon Question 6.3). The choice of parametric versus non-parametric test shall be determined by assessment of normality assumptions using Shapiro-Wilk tests and visual inspection of distributions.

3.7.3.2 Experience Level Comparison

For comparisons across the four experience level categories (Question 6.4), one-way ANOVA or Kruskal-Wallis tests shall be employed as appropriate based upon normality assumptions. Post-hoc pairwise comparisons shall be conducted using Tukey's HSD (for ANOVA) or Dunn's test (for Kruskal-Wallis) to identify specific group differences.

3.7.3.3 Association Analysis

Chi-square tests of independence shall examine associations between categorical variables, such as the relationship between professional field and prior Digital Engineering exposure (Question 1.2), or between experience level and organizational investment willingness (Questions 4.5, 5.7).

3.7.4 Composite Score Analysis

To provide summary measures of awareness and perceived value, composite scores shall be calculated by averaging Likert responses within thematic groupings:

3.7.4.1 Awareness Composite

Average of Question 1.1 and Questions 2.1-2.6 (seven items measuring familiarity and understanding of Digital Engineering capabilities)

3.7.4.2 IT Value Perception Composite

Average of Questions 3.1, 3.3-3.5, and 4.1-4.4 (eight items measuring perceived value of Digital Engineering for IT operations)

3.7.4.3 Security Value Perception Composite

Average of Questions 3.2, 3.6, and 5.1-5.6 (eight items measuring perceived value of Digital Engineering for information assurance and cybersecurity)

Internal consistency of composite scores shall be assessed using Cronbach's alpha, with values above 0.70 considered acceptable for research purposes. If internal consistency proves insufficient, item analysis shall be conducted to identify potentially problematic items.

3.7.5 Statistical Significance and Effect Sizes

Statistical significance shall be evaluated at the $\alpha = 0.05$ level for all inferential tests. However, given the large sample size targeted for this study, effect sizes shall be reported alongside significance tests to assess practical significance of observed differences. Statistical significance alone can mislead when sample sizes are large; effect sizes reveal whether differences matter in practice. Cohen's d shall be reported for group comparisons, with

conventional thresholds of 0.2 (small), 0.5 (medium), and 0.8 (large) used for interpretation. For chi-square tests, Cramér's V shall be reported as the effect size measure.

3.7.6 Management of Type I and Type II Errors

Multiple provisions within the analytical design manage the risk of both Type I errors (false positives—concluding that a difference or association exists when it does not) and Type II errors (false negatives—failing to detect a genuine difference or association). Operating at the levels of sample design, instrument design, and analytical procedure, these provisions

3.7.6.1 Type I Error Management

The primary Type I error concern in this study arises from the conduct of multiple statistical tests across 27 survey items and multiple subgroup comparisons. When numerous tests are performed at the $\alpha = 0.05$ significance level, the family-wise error rate increases, elevating the probability that at least one test produces a spurious significant result. To manage this inflation, the analytical approach employs the Holm-Bonferroni sequential correction procedure for families of related comparisons. The Holm-Bonferroni method provides stronger Type I error control than unadjusted testing while maintaining greater statistical power than the classical Bonferroni correction, which can be overly conservative when applied to large families of tests.

Comparisons are organized into logical families reflecting the research question structure: awareness items (Section 1 and Section 2 questions addressing Research Question 1), applicability items (Section 3 questions bridging Research Questions 2 and 3), IT value items (Section 4 questions addressing Research Questions 2 and 3), and information assurance value items (Section 5 questions addressing Research Questions 2 and 3). Within each family, the Holm-Bonferroni correction adjusts significance thresholds to maintain the family-wise error rate at $\alpha = 0.05$. Cross-family comparisons, such as overall awareness

versus overall perceived value correlations, are treated as planned comparisons evaluated at the unadjusted $\alpha = 0.05$ level, as these represent distinct theoretical questions rather than multiple tests of similar hypotheses.

The emphasis upon effect sizes alongside significance testing provides an additional safeguard against Type I error interpretation. Even when statistical tests yield significant p-values after correction, effect size assessment ensures that observed differences reflect practically meaningful magnitudes rather than trivial differences detected through large sample power.

3.7.6.2 Type II Error Management

Type II error risk is managed primarily through sample size design. The target sample of 385–450 completed responses provides sufficient statistical power to detect meaningful differences in the primary analyses. For the primary descriptive analyses addressing Research Question 1, the sample size ensures that reported proportions and means achieve margins of error within five percentage points at the 95% confidence level, providing adequate precision to characterize awareness levels and value perceptions.

For comparative analyses between professional subgroups, power considerations informed the oversampling target. Assuming an approximately even split between IT and information assurance respondents, each subgroup comprises approximately 190–225 respondents. At these subgroup sizes, independent samples t-tests achieve statistical power exceeding 0.80 to detect medium effect sizes (Cohen's d = 0.5) at $\alpha = 0.05$, consistent with conventional power analysis thresholds recommended for behavioral science research. For smaller effect sizes (Cohen's d = 0.3), power at these subgroup sizes approaches 0.60, which represents a recognized limitation for detecting subtle differences between professional groups. This power limitation is acknowledged and reported alongside subgroup analyses so that non-significant results are interpreted appropriately—as insufficient evidence rather than as evidence of no difference.

For experience level comparisons across four categories, the distribution of respondents across categories may result in unequal cell sizes that reduce power for specific pairwise comparisons. The analytical plan addresses this by reporting confidence intervals for all group means, enabling assessment of overlap and practical significance even when formal tests fail to reach significance. Non-parametric alternatives (Kruskal-Wallis with Dunn's post-hoc test) are employed when distributional assumptions are not met, as these tests maintain appropriate Type II error rates under non-normal conditions.

3.7.6.3 Instrument-Level Error Reduction

Survey instrument design contributes to error management through several structural features. Established five-point Likert scales with validated anchor sets reduce measurement error that could contribute to both Type I and Type II errors by ensuring that response variability reflects genuine differences in perception rather than response format artifacts. Consistent scale formatting across Sections 2 through 5 reduces within-respondent variability attributable to format switching, improving signal-to-noise ratios in comparative analyses.

The inclusion of both broad constructs (overall awareness, overall value perception) and specific sub-constructs (awareness of individual Digital Engineering pillars, value for specific operational domains) enables triangulation of findings. Convergent results across related items strengthen confidence in significant findings (reducing false positive concern), while divergent results prompt examination of whether non-significant findings reflect genuine null effects or insufficient measurement sensitivity (informing Type II error assessment).

Composite score analysis, with internal consistency assessed through Cronbach's alpha, further mitigates measurement error by aggregating multiple indicators of each construct. Composite scores based upon reliable item sets exhibit less measurement error than individual items, improving the precision of group comparisons and reducing Type II error

risk for analyses involving aggregated constructs.

3.8 Reliability and Validity Considerations

3.8.1 Content Validity

Content validity was established through systematic mapping of survey questions to research questions and through alignment with established frameworks in the Digital Engineering and technology acceptance literature. The survey instrument structure directly addresses the four pillars of Digital Engineering—MBSE, the Digital Thread, Digital Twin, and PLM—as established by INCOSE and adopted by NASA, DoD, and the Intelligence Community. Questions were reviewed to ensure they accurately represent the constructs of interest and employ appropriate professional terminology familiar to IT and information assurance practitioners.

3.8.2 Construct Validity

Construct validity is supported through use of established question formats and scale anchors drawn from validated instruments in technology acceptance research. Following conventions from TAM and UTAUT research, the agreement scale format has demonstrated validity for measuring technology perceptions across diverse populations. A tripartite structure examining awareness, applicability, and perceived value follows established patterns in technology adoption research that have proven effective across multiple domains.

3.8.3 Reliability

Internal consistency reliability shall be assessed for composite scores using Cronbach's alpha. Additionally, the standardized question format and scale anchors across sections support response consistency by presenting respondents with familiar response frameworks

throughout the survey. The use of consistent Likert scale response options across Sections 2-5 reduces potential confusion and supports reliable responding.

3.8.4 Pilot Testing and Instrument Refinement

Prior to formal dissertation proposal development, the survey instrument underwent pilot testing during the Spring 2024 semester. An earlier version of the instrument was administered to IT and information assurance professionals, serving multiple purposes: evaluating question clarity and comprehension among respondents representative of the target population, assessing completion time and respondent fatigue, identifying ambiguous or confusing question formulations, and generating preliminary data to inform the structural design and thematic organization of the final instrument.

Data collected during the pilot study provided empirical evidence that directly shaped the design and structure of the survey questions presented in this methodology. Pilot results informed several consequential design decisions reflected in the current instrument. Question wording was refined to reduce ambiguity in how Digital Engineering concepts were described, balancing the competing requirements of providing sufficient context for respondents unfamiliar with Digital Engineering terminology while avoiding language that could prime respondents toward particular response patterns. Section ordering was adjusted based upon pilot completion patterns to place awareness questions before value assessment questions, establishing a cognitive progression from recognition through evaluation. The pilot also validated the estimated completion time and confirmed that the five-point Likert scale format produced adequate response distribution across scale points without floor or ceiling effects.

The pilot study's contribution extends beyond instrument refinement to substantive validation of the research premise. Pilot data confirmed that the target population includes substantial variation in Digital Engineering awareness levels, validating the foundational assumption that awareness and perceived value remain open empirical questions re-

quiring investigation. The observed variance in pilot responses across both awareness and value dimensions confirmed that the instrument captures meaningful differences among respondents rather than producing uniform response distributions that would limit analytical value.

The pilot testing process complemented the content validity established through systematic mapping of survey questions to research questions and alignment with established Digital Engineering and technology acceptance frameworks. Where the content validity process ensured that the instrument measures the intended constructs, pilot testing confirmed that respondents interpret questions as intended and can provide meaningful responses within the designed format. The combination of theoretical grounding through framework alignment and empirical refinement through pilot testing strengthens confidence in the instrument's ability to generate valid, reliable data addressing the research questions.

3.8.5 Limitations

Several limitations should be considered when interpreting study results:

- The non-probability sampling approach limits generalizability to the broader population of IT and information assurance professionals. Results should be interpreted as indicative of perceptions within the accessible population rather than definitive measures of the entire professional community.

- Self-selection bias may result in over-representation of professionals with existing awareness or interest in Digital Engineering. Individuals who recognize the term or possess prior exposure may be more likely to complete the survey, potentially inflating reported awareness levels.

- Social desirability bias may influence responses, particularly regarding perceived value questions. Respondents may indicate greater perceived value than they gen-

uinely hold if they believe Digital Engineering represents a progressive or professionally desirable position.

- Self-reported awareness and perceptions may not accurately reflect actual knowledge or organizational capabilities. Respondents may overestimate their familiarity with Digital Engineering concepts or underestimate existing capabilities within their organizations that align with Digital Engineering principles but employ different terminology.

- The cross-sectional design captures perceptions at a single point in time during a period of rapid evolution in both Digital Engineering practices and enterprise IT methodologies. Results represent a temporal snapshot that may not reflect awareness levels or perceptions six months or a year following data collection, particularly given increasing industry attention to digital transformation initiatives.

- Non-target respondents who complete the survey may affect results, though demographic questions enable identification and potential exclusion of responses from outside the target population.

- The survey measures perceived value and anticipated benefits rather than actual experienced benefits. Positive perceptions do not guarantee that Digital Engineering would deliver value if implemented, nor do they indicate organizational readiness for adoption.

3.8.6 Response Bias Mitigation

Several design decisions embedded within the survey instrument and recruitment strategy proactively mitigate identified sources of response bias. These measures complement the acknowledged limitations by reducing their anticipated impact upon data quality and interpretive validity.

Self-selection bias, whereby respondents with prior Digital Engineering awareness disproportionately choose to participate, is mitigated through recruitment messaging that explicitly frames the survey as targeting all IT and information assurance professionals regardless of Digital Engineering familiarity. Recruitment materials emphasize that the research seeks perspectives from professionals across the awareness spectrum and that no prior knowledge of Digital Engineering is required or expected. This framing encourages participation from professionals who might otherwise self-exclude upon encountering unfamiliar terminology.

Survey questions in Sections 2 through 5 incorporate minimal contextual descriptions of Digital Engineering capabilities within the question stems. Reflecting a deliberate balance between two competing methodological concerns, this design choice On one hand, questions devoid of contextual information would measure only pre-existing awareness, excluding respondents unfamiliar with Digital Engineering terminology from providing meaningful responses about perceived value. On the other hand, extensive descriptions risk priming respondents toward positive assessments. The instrument resolves this tension by providing sufficient context for respondents to form an informed judgment about each capability statement without advocating for or characterizing the capability in evaluative terms. Each question describes what a Digital Engineering capability does in neutral, functional language, enabling respondents to assess whether that function would provide value within their professional context based upon their own domain expertise. This approach ensures that respondents unfamiliar with Digital Engineering terminology are not confused by questions referencing concepts they have not encountered, while avoiding framing that suggests a preferred response direction.

Social desirability bias is mitigated through the anonymous survey design, which removes professional reputation concerns that might otherwise influence responses. The absence of personally identifiable information collection, combined with clear communication of anonymity protections in the informed consent notice, encourages candid responses

about knowledge gaps and skepticism toward unfamiliar methodologies.

Acquiescence bias, the tendency for respondents to agree with statements regardless of content, is addressed through the inclusion of the neutral midpoint option in Likert scale responses. The "Neither agree nor disagree" response enables genuine expression of uncertainty or indifference rather than forcing agreement or disagreement. Additionally, the binary and ternary response options for investment willingness questions (Questions 4.5 and 5.7) include an "Unsure" option that captures genuine uncertainty without channeling indecisive respondents toward affirmative responses.

Wave analysis comparing early and late respondents shall be conducted during data analysis to assess whether response patterns differ systematically between initial and subsequent response waves. Significant differences between early and late respondents may indicate non-response bias, as late respondents are often considered more representative of non-respondents. Demographic composition of the sample shall be compared against known characteristics of the IT and information assurance professional population to assess representativeness, with any identified disparities reported as potential limitations on generalizability.

An additional analytical safeguard enables post-hoc assessment of potential priming effects from the contextual descriptions embedded in survey questions. Comparison of value perception scores (Sections 4 and 5) between respondents reporting high Digital Engineering familiarity (Question 1.1 scores of four or five) and those reporting low familiarity (scores of one or two) provides a diagnostic for priming influence. If both familiarity groups report similarly elevated perceived value, the priming hypothesis gains support, suggesting that question descriptions may have influenced responses independent of prior knowledge. If high-familiarity respondents report substantially higher perceived value than low-familiarity respondents, the measurements more likely reflect genuine perception differences informed by prior knowledge and professional experience rather than question framing effects. This comparison does not eliminate priming concerns but provides em-

pirical evidence for assessing their magnitude and interpretive implications.

3.9 Ethical Considerations

This research was designed in accordance with ethical principles for human subjects research and submitted for review and comment by the Dakota State University Institutional Review Board (IRB); approval by the IRB shall proceed after Dissertation Proposal Defense completion. Key ethical considerations include:

3.9.1 Anonymity

The survey collects no personally identifiable information, ensuring respondent anonymity. Demographic questions are limited to professional field and experience level, which cannot identify individual respondents.

3.9.1.1 Voluntary Participation

Participation is voluntary with no consequences for non-participation. Respondents may exit the survey at any time before submission without consequence and may skip any questions they choose not to answer.

3.9.1.2 Minimal Risk

The research presents minimal risk to participants, with potential inconvenience limited to time required for survey completion. Risks are similar to those encountered in normal daily internet activity.

3.9.1.3 Informed Consent

Informed consent is obtained through the participation notice presented before survey questions, with submission constituting consent.

3.9.1.4 Data Protection

Data shall be stored securely using password protection, multifactor authentication, and encryption at rest and in transit. Data shall be used solely for research purposes as described in the participation notice.

3.9.1.5 Data Use Restrictions

Survey raw data shall not be sold or used for any purpose other than the dissertation research.

3.10 Research Timeline and Project Schedule

This research follows a structured implementation plan spanning approximately twenty-two months from dissertation committee formation through final defense. Aligned with Dakota State University's doctoral program requirements and academic calendar, the timeline accommodates the iterative nature of quantitative survey research. Each phase builds systematically upon preceding work, ensuring adequate time for committee review, institutional oversight, data collection, and rigorous analysis. Figure 3.12 presents the project schedule as a gantt chart.

3.10.1 Phase 1: Committee Formation and Preparation (May 2025 – August 2025)

The initial phase established the dissertation committee and governance structure for the research project. During this period, the candidate identified and invited faculty members with relevant expertise. Committee formation required consideration of faculty availability, disciplinary expertise alignment with the research questions, and institutional requirements for committee composition. Preliminary discussions with committee mem-

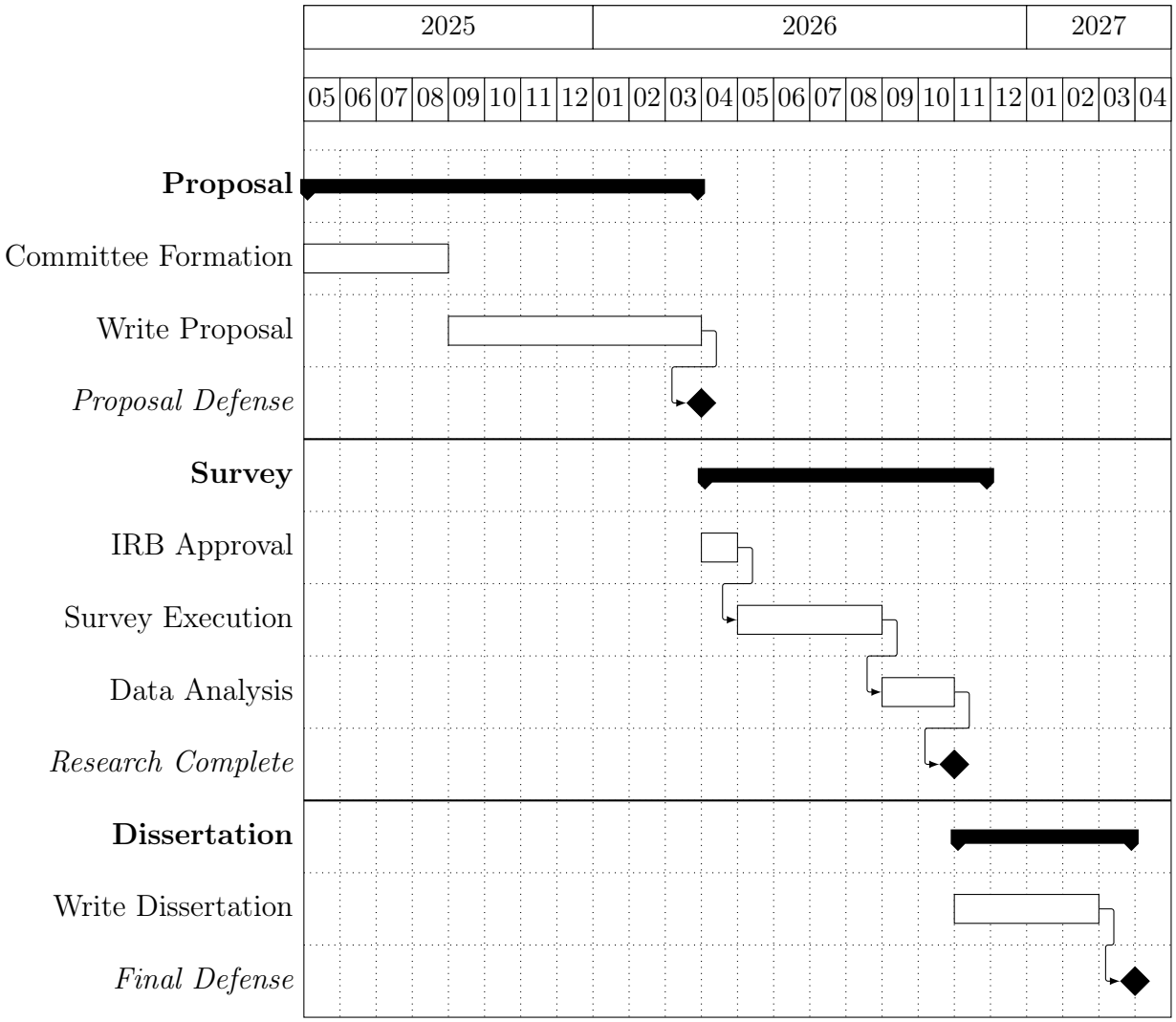


Figure 3.12: Dissertation Timeline

bers addressed research scope, methodology, and expected timeline. Committee formation concluded in August 2025, enabling proposal development under appropriate faculty guidance.

3.10.2 Phase 2: Dissertation Proposal Development (September 2025 – February 2026)

The proposal development phase spans six months, reflecting the iterative nature of academic research design. During September and October 2025, the candidate completed

initial proposal research and draft concepts encompassing the problem statement, literature review, research questions, and detailed methodology. These drafts underwent review by the dissertation chair, with feedback informing subsequent revisions. November 2025 through February 2026 involves iterative refinement based upon committee member feedback, addressing conceptual clarity, methodological rigor, literature synthesis, and alignment between research questions and analytical approaches. February 2026 focuses upon final proposal preparation, incorporating all committee feedback and ensuring compliance with Dakota State University formatting and content requirements.

3.10.3 Phase 3: Proposal Defense and IRB Approval (March 2026 – April 2026)

Scheduled for March 2026, the dissertation proposal defense provides the committee opportunity to evaluate the research design before data collection commences. Addressing the research problem, theoretical framework, methodology, and anticipated contributions, the defense presentation Successful defense results in committee approval to proceed with human subjects research application, with any required modifications addressed immediately thereafter.

Following successful proposal defense, the candidate submits the Institutional Review Board application for human subjects research approval. Included within the IRB application are the complete research protocol, survey instrument, recruitment materials, informed consent procedures, and data protection plan. April 2026 is allocated for IRB review and approval, recognizing that no participant recruitment or data collection may commence without formal IRB authorization.

3.10.4 Phase 4: Survey Execution (May 2026 – August 2026)

The survey execution phase spans four months, enabling comprehensive recruitment across multiple professional channels and providing adequate response time for participants. May 2026 focuses upon survey platform configuration, recruitment material distribution, and initial participant engagement through professional networks and industry associations. June and July 2026 constitute the active data collection period, with ongoing monitoring of response rates, data quality, and sample composition. This extended collection period accommodates the schedules of working professionals who constitute the target population. August 2026 serves as a buffer period for late responses and final data collection activities, allowing for additional recruitment waves if initial response rates prove insufficient to achieve the target sample size of 385–450 completed surveys.

3.10.5 Phase 5: Data Analysis (September 2026 – November 2026)

The data analysis phase requires three months to conduct thorough examination of survey results addressing all three research questions. September 2026 focuses upon data preparation, cleaning, and preliminary descriptive analysis, including response validation, missing data assessment, and calculation of basic descriptive statistics for all survey questions. October 2026 addresses the primary analyses required to answer each research question: comparative analyses across professional subgroups, composite score calculation and reliability assessment, and inferential statistical testing. November 2026 involves interpretation of results, identification of key findings, and preparation of tables and figures for the results chapter.

3.10.6 Phase 6: Dissertation Writing and Defense (December 2026 – March 2027)

The dissertation writing phase spans three months. While Chapters 1 through 3 exist in proposal form, they require revision to reflect any modifications made during proposal defense and data collection. Chapters 4 and 5 must be written to present results and discuss their implications. December 2026 focuses upon completing the results chapter, presenting findings organized by research question with appropriate statistical support. January 2027 addresses the discussion chapter, interpreting results in the context of existing literature, addressing research limitations, and proposing future research directions. February 2027 involves comprehensive revision of all chapters and submission of the complete dissertation to the committee.

Occurring in March 2027, approximately twenty-two months after the research project commenced, the dissertation final defense marks the culmination of the research effort. A defense presentation summarizing the complete research project emphasizes key findings and their significance for Digital Engineering adoption in Information Assurance and IT Service Management contexts. Successful defense leads to degree conferral following any required minor revisions, positioning the candidate for degree completion during the spring 2027 term.

3.11 Chapter Summary

This chapter has presented the research methodology employed to investigate professional awareness and perceptions of Digital Engineering capabilities among IT and information assurance professionals. Employing a quantitative survey methodology, the research follows a systems engineering lifecycle approach that ensures rigor and traceability throughout the research process. Refined through pilot testing conducted during the

Spring 2024 semester, the survey instrument systematically addresses the three research questions through 27 questions organized into six thematic sections covering awareness, understanding, applicability, and perceived value for both IT and information assurance domains.

A target sample of 385-450 completed responses shall provide sufficient statistical power to achieve a maximum margin of error of five percent at the 95% confidence level. Data analysis shall employ descriptive statistics to characterize awareness levels and value perceptions, with comparative analyses examining differences across professional subgroups and experience levels. Composite scores shall summarize overall awareness and value perceptions with internal consistency assessed through Cronbach's alpha. The analytical plan addresses the ordinal-interval debate surrounding Likert scale data through dual-reporting of parametric and non-parametric summaries, and manages Type I error inflation from multiple comparisons through the Holm-Bonferroni sequential correction procedure applied within logical families of related tests.

Proactive response bias mitigation is incorporated through recruitment messaging designed to encourage participation across the awareness spectrum, survey question design that provides minimal contextual information sufficient for informed response without evaluative priming, and planned wave analysis to assess non-response bias. Complementing the acknowledged limitations of non-probability sampling and self-selection, these provisions strengthen confidence in the validity of collected data.

Establishing a rigorous foundation, the methodology generates empirical evidence regarding professional perceptions of Digital Engineering that can inform future research and practice in information assurance and IT service delivery. A systems engineering approach to research design ensures traceability between research questions, survey instruments, and analytical approaches—demonstrating disciplinary rigor of the research.

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] 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/

[4] 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

[5] 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.

[6] 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

[7] 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

[8] B. Bokan and J. Santos, "Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures," in *2021 Systems and In-*

formation Engineering Design Symposium (SIEDS), IEEE, 2021, pp. 1–6. DOI: 10.1109/SIEDS52267.2021.9483736

[9] International Organization for Standardization, "ISO 31000:2018 Risk Management — Guidelines," International Organization for Standardization, Standard, 2018. [Online]. Available: https://www.iso.org/standard/65694.html

[10] 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

[11] 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.

[12] 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

[13] National Institute of Standards and Technology, "The NIST cybersecurity framework (CSF) 2.0," National Institute of Standards and Technology, Tech. Rep., Feb. 2024, NIST Cybersecurity White Paper (CSWP) 29. DOI: 10.6028/NIST.CSWP.29 [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29

[14] R. Ross and V. Pillitteri, "Protecting controlled unclassified information in nonfederal systems and organizations," National Institute of Standards and Technology, NIST Special Publication 800-171 Revision 3, 2024. DOI: 10.6028/NIST.SP.800-171r3

[15] 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

[16] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid, "Enhanced security requirements for protecting controlled unclassified information: A supplement to NIST special publication 800-171," National Institute of Standards and Technology, NIST Special Publication 800-172, 2021. DOI: 10.6028/NIST.SP.800-172

[17] Department of Defense, "Cybersecurity maturity model certification (CMMC) program," Department of Defense, 32 CFR Part 170, Final Rule, 2024, Published October 15, 2024; effective December 16, 2024.

[18] Gartner, *Why CMDB Projects Fail and How to Avoid Their Mistakes*, Gartner Research, 2019. Accessed: Jan. 3, 2026. [Online]. Available: https://www.gartner.com/en/documents/3970851

[19] 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

[20] Gartner, *Shadow IT: The Risks and How to Manage Them*, Gartner Research, 2022. Accessed: Jan. 3, 2026. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/shadow-it

[21] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2024," IBM Corporation, Research Report, Jul. 2024. Accessed: Jan. 9, 2026. [Online]. Available: https://www.ibm.com/reports/data-breach

[22] 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

[23] 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

[24] 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

[25] E. B. Rogers and S. W. Mitchell, "MBSE Delivers Significant Return on Investment in Evolutionary Development of Complex SoS," *Systems Engineering*, vol. 24, no. 6, pp. 385–408, 2021. DOI: 10.1002/sys.21592 [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/full/10.1002/sys.21592

[26] 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

[27] 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

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

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

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

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

[32] 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

[33] 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.

[34] 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/

[35] 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

[36] 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

[37] 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

[38] 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

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

[40] International Organization for Standardization, "ISO 23247: Automation Systems and Integration – Digital Twin Framework for Manufacturing," International Organization for Standardization, Standard, 2021. [Online]. Available: https://www.iso.org/standard/75066.html

[41] 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

[42] IETF Network Management Research Group, *Network Digital Twin Architecture*, Internet-Draft, 2024. Accessed: Jan. 3, 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-nmrg-network-digital-twin-arch/

[43] 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

[44] 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

[45] 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/

[46] 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/

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

[48] S. Gil, P. H. Mikkelsen, C. Gomes, and P. G. Larsen, "Survey on open-source digital twin frameworks — a case study approach," *Software: Practice and Experience*, vol. 54, no. 6, pp. 929–960, DOI: https://doi.org/10.1002/spe.3305 eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/spe.3305.

[49] 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

[50] 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

[51] J. Campos, J. Kortelainen, and E. Jantunen, "Industrial Open Source Solutions for Product Life Cycle Management," *Cogent Engineering*, vol. 1, no. 1, pp. 1–15, Aug. 2014. DOI: 10.1080/23311916.2014.939737

[52] 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

[53] 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

[54] 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

[55] 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

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

[57] 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

[58] 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

[59] 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/

[60] 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

[61] 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/

[62] 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

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

[64] 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

[65] 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

[66] J. Bankauskaite, "Comparative Analysis of Enterprise Architecture Frameworks," in *CEUR workshop proceedings IVUS 2019 international conference on information technologies: proceedings of the international conference on information technologies, Kaunas, Lithuania*, CEUR-WS, vol. 2470, Apr. 2019, pp. 61–64. Accessed: Jan. 3, 2025. [Online]. Available: https://ceur-ws.org/Vol-2470/p19.pdf

[67] 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

[68] 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

[69] N. Liu, J. Wang, Y. Zhang, D. Li, and M. Ju, "Top-down military system-of-systems design using MBSE based on UAF: A case study," in *Complex Systems Design & Management*, D. Krob, L. Li, X. Zhang, J. Yao, and M. Guo, Eds., Singapore: Springer Nature Singapore, 2023, pp. 210–219, ISBN: 978-981-99-6511-3. DOI: 10.1007/978-981-99-6511-3_19

[70] 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

[71] 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

[72] 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

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

[74] K. Henderson, T. McDermott, and A. Salado, "MBSE Adoption Experiences in Organizations: Lessons Learned," *Systems Engineering*, vol. 27, no. 1, pp. 214–239, 2024. DOI: 10.1002/sys.21717 Accessed: Nov. 11, 2025.

[75] C. J. Call et al., "The Effects of the Assessed Perceptions of MBSE on Adoption," *INCOSE International Symposium*, vol. 34, no. 1, pp. 358–373, 2024. DOI: 10.1002/iis2.13157 [Online]. Available: https://incose.onlinelibrary.wiley.com/doi/10.1002/iis2.13157

[76] 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

[77] T. A. Chick, S. Pavetti, and N. Shevchenko, "Using Model-Based Systems Engineering (MBSE) to Assure a DevSecOps Pipeline," Carnegie Mellon University Software Engineering Institute, Technical Report CMU/SEI-2023-TR-001, 2023. [Online]. Available: https://www.sei.cmu.edu/documents/6140/Using_MBSE_to_Assure_DevSecOps_Pipelines.pdf

[78] 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.

[79] A. M. Madni and M. Sievers, "Model-Based Systems Engineering: Motivation, Current Status, and Research Opportunities," *Systems Engineering*, vol. 21, no. 3, pp. 172–190, 2018. DOI: 10.1002/sys.21438

[80] 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 Accessed: Jan. 3, 2026. [Online]. Available: https://www.mdpi.com/2079-8954/13/12/1046

[81] 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

[82] 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

[83] 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

[84] D. R. Call and D. R. Herber, "Applicability of the Diffusion of Innovation Theory to Accelerate Model-Based Systems Engineering Adoption," *Systems Engineering*, vol. 25, no. 6, pp. 574–583, 2022. DOI: 10.1002/sys.21638

[85] K. Henderson and A. Salado, "The Effects of Organizational Structure on MBSE Adoption in Industry: Insights from Practitioners," *Engineering Management Journal*, vol. 36, no. 1, pp. 117–143, 2024. DOI: 10.1080/10429247.2023.2210494 Accessed: Jan. 3, 2026.

[86] A. Vogelsang, T. Amorim, F. Pudlitz, P. Gersing, and J. Philipps, "Should I Stay or Should I Go? On Forces that Drive and Prevent MBSE Adoption in the Embedded Systems Industry," in *Product-Focused Software Process Improvement (PROFES 2017)*, ser. Lecture Notes in Computer Science, vol. 10611, Springer, 2017, pp. 182–198. DOI: 10.1007/978-3-319-69926-4_14

[87] 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

[88] M. A. Bone, M. R. Blackburn, D. H. Rhodes, D. N. Cohen, and J. A. Guerrero, "Transforming Systems Engineering Through Digital Engineering," *The Journal of Defense Modeling and Simulation*, vol. 16, no. 4, pp. 339–355, 2019. DOI: 10.1177/1548512917751873

[89] J. Huff, H. Medal, and K. Griendling, "A Model-Based Systems Engineering Approach to Critical Infrastructure Vulnerability Assessment and Decision Analysis," *Systems Engineering*, vol. 22, no. 3, pp. 214–231, 2019. DOI: 10.1002/sys.21460

[90] D. Mažeika and R. Butleris, "Integrating Security Requirements Engineering into MBSE: Profile and Guidelines," *Security and Communication Networks*, vol. 2020, pp. 1–12, 2020. DOI: 10.1155/2020/5137625

[91] 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

[92] P. H. Nguyen, S. Ali, and T. Yue, "Model-Based Security Engineering for Cyber-Physical Systems: A Systematic Mapping Study," *Information and Software Technology*, vol. 83, pp. 116–135, 2017. DOI: 10.1016/j.infsof.2016.11.004

[93] M. El-Hajj, T. Itäpelto, and T. Gebremariam, "Systematic Literature Review: Digital Twins' Role in Enhancing Security for Industry 4.0 Applications," *Security and Privacy*, vol. 7, no. 5, e396, 2024. DOI: 10.1002/spy2.396

[94] N. Alhumam et al., "A Comprehensive Review on Cybersecurity of Digital Twins: Issues, Challenges, and Future Research Directions," *IEEE Access*, vol. 13, pp. 1–25, 2025. DOI: 10.1109/ACCESS.2025.3545004

[95] 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

[96] 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

[97] 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

[98] 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

[99] C. Alcaraz and J. Lopez, "Digital twin: A comprehensive survey of security threats," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1475–1503, 2022. DOI: 10.1109/COMST.2022.3171465

[100] S. Suhail, M. Iqbal, and R. Jurdak, "The perils of leveraging evil digital twins as security-enhancing enablers," *Communications of the ACM*, vol. 67, no. 1, pp. 39–42, 2024. DOI: 10.1145/3631539

[101] S. Suhail, M. Iqbal, R. Hussain, and R. Jurdak, "ENIGMA: An explainable digital twin security solution for cyber-physical systems," *Computers in Industry*, vol. 151, p. 103 961, 2023. DOI: 10.1016/j.compind.2023.103961

[102] C. Rodrigues, W. S. S. Júnior, W. Oliveira, and I. Lima, "A data rate monitoring approach for cyberattack detection in digital twin communication," *Sensors*, vol. 25, no. 24, p. 7476, 2025. DOI: 10.3390/s25247476

[103] C. Gehrmann and M. Gunnarsson, "A digital twin based industrial automation and control system security architecture," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 669–680, 2020. DOI: 10.1109/TII.2019.2938885

[104] M. Eckhart, B. Brenner, A. Ekelhart, and E. Weippl, "Security-enhancing digital twins: Characteristics, indicators, and future perspectives," *IEEE Security & Privacy*, vol. 21, no. 6, pp. 64–75, 2023. DOI: 10.1109/MSEC.2023.3271225

[105] 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

[106] 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

[107] H. Haverinen et al., "Automating cybersecurity compliance in DevSecOps with open information model for security as code," in *Proceedings of the 4th Eclipse Security, AI, Architecture and Modelling Conference on Data Space (SEAAM '24)*, ACM, 2024. DOI: 10.1145/3685651.3686700

[108] R. Chandramouli, "Strategies for the integration of software supply chain security in DevSecOps CI/CD pipelines," National Institute of Standards and Technology, NIST Special Publication 800-204D, 2024. DOI: 10.6028/NIST.SP.800-204D

[109] K. P. Joshi, L. Elluri, and A. Nagar, "An Integrated Knowledge Graph to Automate Cloud Data Compliance," *IEEE Access*, vol. 8, pp. 148 541–148 555, 2020. DOI: 10.1109/ACCESS.2020.3008964

[110] C. Banse, I. Kunz, A. Schneider, and K. Weiss, "Cloud Property Graph: Connecting Cloud Security Assessments with Static Code Analysis," in *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, IEEE, 2021, pp. 13–19. DOI: 10.1109/CLOUD53861.2021.00014

[111] M. Stojkov, N. Dalčeković, B. Markoski, B. Milosavljević, and G. Sladić, "Towards Cross-Standard Compliance Readiness: Security Requirements Model for Smart Grid," *Energies*, vol. 14, no. 21, p. 6862, 2021. DOI: 10.3390/en14216862

[112] I. Koufos, M. Christopoulou, G. Xilouris, M.-A. Kourtis, M. Souvalioti, and P. Trakadas, "Towards the Automation of Attack Graph-Based Risk Assessment with OSCAL," in *Distributed Computing and Artificial Intelligence, Special Sessions I (DCAI 2024)*, ser. Lecture Notes in Networks and Systems, vol. 1198, Springer, 2025, pp. 319–328. DOI: 10.1007/978-3-031-76459-2_30

[113] R. N. Rajapakse, M. Zahedi, M. A. Babar, and H. Shen, "Challenges and Solutions When Adopting DevSecOps: A Systematic Review," *Information and Software Technology*, vol. 141, p. 106 700, 2022. DOI: 10.1016/j.infsof.2021.106700

[114] H. Myrbakken and R. Colomo-Palacios, "DevSecOps: A Multivocal Literature Review," in *Software Process Improvement and Capability Determination (SPICE 2017)*, ser. Communications in Computer and Information Science, vol. 770, Springer, 2017, pp. 17–29. DOI: 10.1007/978-3-319-67383-7_2

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

[116] 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

[117] 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

[118] Gartner, *CMDB Data Quality: Critical Success Factors*, Gartner Research, 2020. Accessed: Oct. 21, 2025. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/cmdb-configuration-management-database

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

[120] 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

[121] 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/

[122] 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/

[123] 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

[124] S. Klotz, A. Kopper, M. Westner, and S. Strahringer, "Causing Factors, Outcomes, and Governance of Shadow IT and Business-Managed IT: A Systematic Literature Review," *International Journal of Information Systems and Project Management*, vol. 7, no. 1, pp. 15–43, 2019. DOI: 10.12821/ijispm070102

[125] D. Fürstenau, H. Rothe, and M. Sandner, "Leaving the Shadow: A Configurational Approach to Explain Post-Identification Outcomes of Shadow IT Systems," *Business & Information Systems Engineering*, vol. 63, no. 2, pp. 97–111, 2021. DOI: 10.1007/s12599-020-00635-2

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

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

[128] 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.

[129] 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

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

[131] Ivanti, "State of Cybersecurity Trends Report 2025," Ivanti, Research Report, 2025. Accessed: Jan. 9, 2026. [Online]. Available: https://www.ivanti.com/resources/research-reports/state-of-cybersecurity-report

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

[133] 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

[134] 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

[135] 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

[136] 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

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

[138] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2025," IBM Corporation, Research Report, 2025. Accessed: Jan. 9, 2026. [Online]. Available: https://www.ibm.com/reports/data-breach

[139] 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

[140] J. Beese, S. Aier, K. Haki, and R. Winter, "The Impact of Enterprise Architecture Management on Information Systems Architecture Complexity," *European Journal of Information Systems*, vol. 32, no. 6, pp. 1070–1090, 2023. DOI: 10.1080/0960085X.2022.2103045

[141] S. Kotusev, "Enterprise Architecture and Enterprise Architecture Artifacts: Questioning the Old Concept in Light of New Findings," *Journal of Information Technology*, vol. 34, no. 2, pp. 102–128, 2019. DOI: 10.1177/0268396218816273

[142] S. Kurnia, S. Kotusev, G. Shanks, R. Dilnutt, and S. Milton, "Stakeholder Engagement in Enterprise Architecture Practice: What Inhibitors Are There?" *Information and Software Technology*, vol. 134, p. 106 536, 2021. DOI: 10.1016/j.infsof.2021.106536

[143] 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: doi.org/10.22495/jgrv11i2siart15

[144] 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

[145] L. Mendes, C. Cerdeiral, and G. Santos, "Documentation technical debt: A qualitative study in a software development organization," in *Proceedings of the XXXIII Brazilian Symposium on Software Engineering*, ser. SBES '19, ACM, 2019, pp. 447–451. DOI: 10.1145/3350768.3350773

[146] 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

[147] H. J. Junior and G. H. Travassos, "Consolidating a common perspective on technical debt and its management through a tertiary study," *Information and Software Technology*, vol. 149, p. 106 964, 2022, ISSN: 0950-5849. DOI: https://doi.org/10.1016/j.infsof.2022.106964 Accessed: Mar. 15, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0950584922001057

[148] 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

[149] 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

[150] 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

[151] D. A. Dillman, J. D. Smyth, and L. M. Christian, *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*, 4th. Hoboken, NJ: John Wiley & Sons, 2014, ISBN: 978-1118456149.

[152] W. Fan and Z. Yan, "Factors Affecting Response Rates of the Web Survey: A Systematic Review," *Computers in Human Behavior*, vol. 26, no. 2, pp. 132–139, 2010. DOI: 10.1016/j.chb.2009.10.015

[153] S. Jamieson, "Likert scales: How to (ab)use them," *Medical Education*, vol. 38, no. 12, pp. 1217–1218, 2004. DOI: 10.1111/j.1365-2929.2004.02012.x

[154] G. Norman, "Likert scales, levels of measurement and the "laws" of statistics," *Advances in Health Sciences Education*, vol. 15, no. 5, pp. 625–632, 2010. DOI: 10.1007/s10459-010-9222-y

[155] G. M. Sullivan and A. R. Artino, "Analyzing and interpreting data from Likert-type scales," *Journal of Graduate Medical Education*, vol. 5, no. 4, pp. 541–542, 2013. DOI: 10.4300/JGME-5-4-18

[156] J. C. F. de Winter and D. Dodou, "Five-point Likert items: T test versus Mann-Whitney-Wilcoxon," *Practical Assessment, Research, and Evaluation*, vol. 15, no. 11, pp. 1–12, 2010. DOI: 10.7275/bj1p-ts64

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?

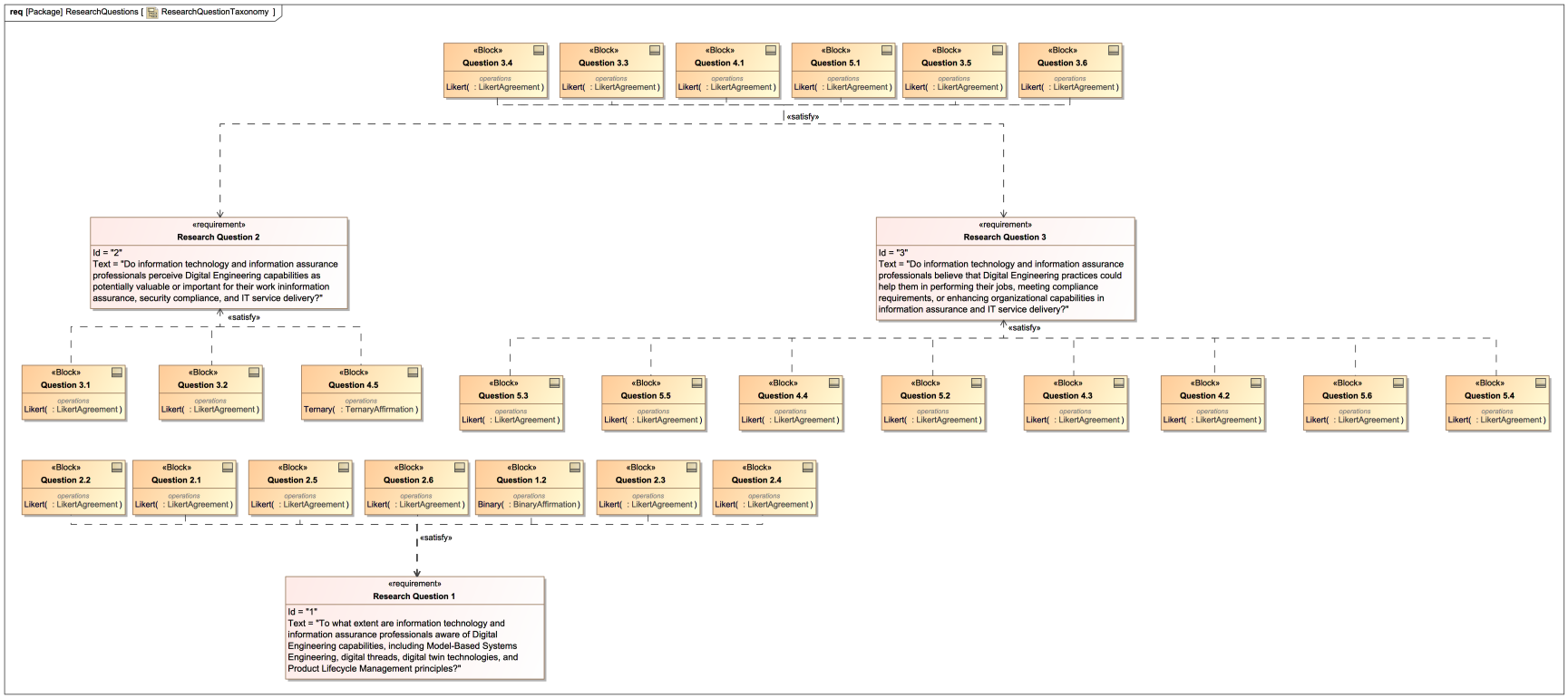


Figure A.1: Research Question Traceability Taxonomy

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

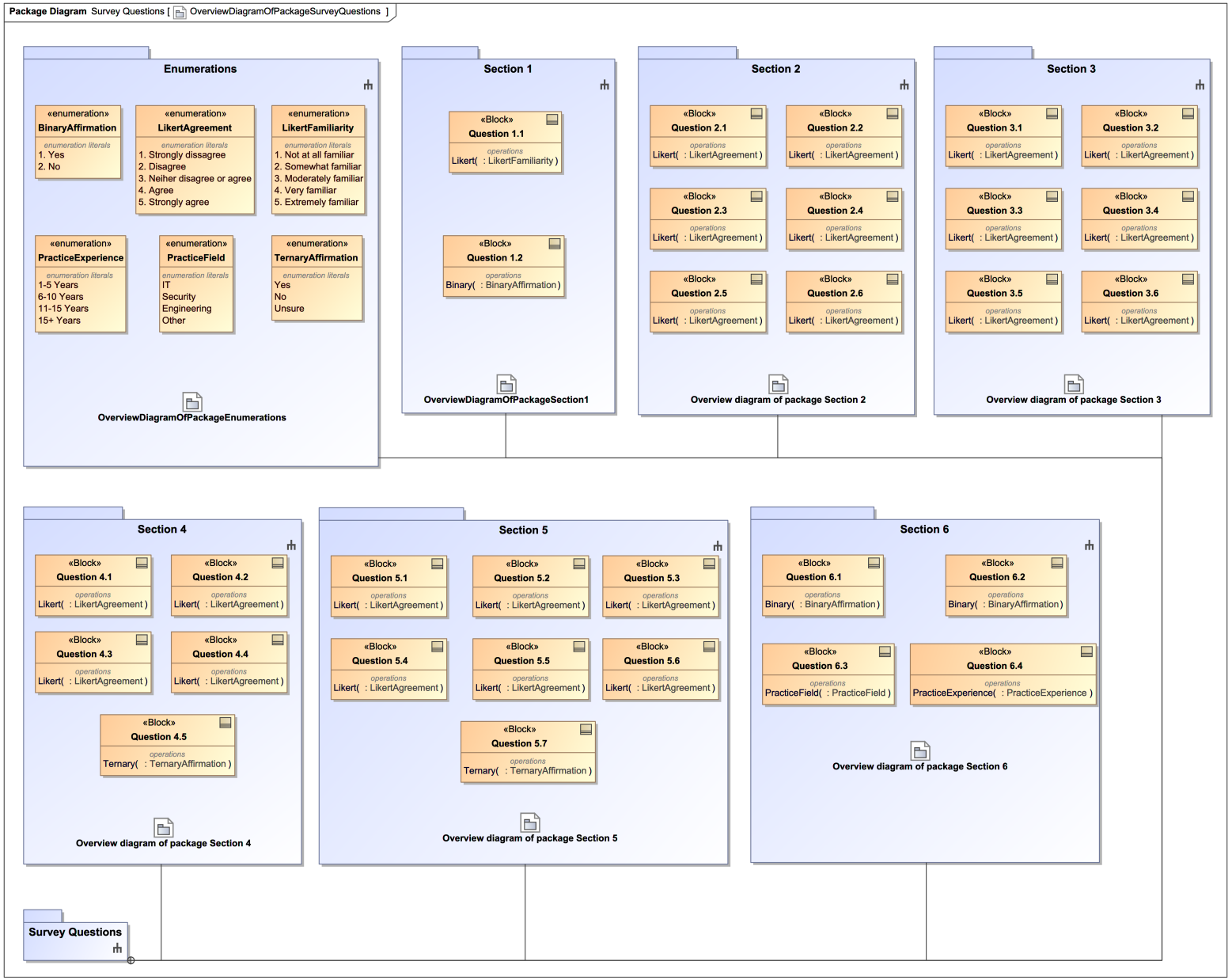


Figure A.2: Taxonomy of Survey Questions

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

Core Dimension: Awareness

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.3.1 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

Core Dimension: Awareness

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.4.1 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

Core Dimension: Applicability

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.5.1 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

Core Dimension Perceived Value (IT Domain)

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.6.1 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

Core Dimension: Perceived Value (Information Assurance Domain)

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.7.1 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

Core Dimension: Supporting/Demographics

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.8.1 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	10
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
16+ 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 & Sonnet 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.