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 07, 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

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. We have the watch, rest well in those green lands upon distant shores

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

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

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

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

Revision History . . . . **ii**

Dissertation Approval Form . . . . **iii**

Acknowledgments . . . . **iv**

Abstract . . . . **v**

Declaration . . . . **vi**

Table of Contents . . . . **vii**

List of Tables . . . . **xv**

List of Figures . . . . **xvi**

Chapter 1:

Introduction **1**

1.1 Current State of Information System Management 3

1.1.1 Information Assurance Practice 4

1.1.2 IT Service Management Practice 6

1.1.3 Challenges in Current Practice 7

1.2 Digital Engineering as Potential Solution 9

1.2.1 Model-Based Systems Engineering 10

1.2.2 Digital Threads 12

1.2.3 Digital Twin 13
1.2.4 Product Lifecycle Management 14
1.3 Gaps in Current Practice 16
1.3.1 Information Assurance Challenges 16
1.3.2 IT Service Management Challenges 17
1.3.3 The Documentation-Reality Gap 18
1.4 Research Questions 19
1.5 Research Scope and Approach 21
1.5.1 Methodological Approach 21
1.5.2 Target Population and Broader Application 22
1.5.3 Potential Benefits for Organizations Serving Underrepresented Populations 23
1.5.4 Why Perceptions Matter 24
1.5.5 Contribution of Prior Research 25
1.6 Significance of the Research 26
1.6.1 Academic Significance 26
1.6.2 Industry Significance 27
1.6.3 Commonwealth Significance 27
1.6.4 Societal Significance 28
1.7 Chapter Summary 29

Chapter 2:

Literature Review 32

2.1 Enterprise Architecture Frameworks 32
2.1.1 The Unified Architecture Framework 33
2.1.2 Department of Defense Architecture Framework 36
2.1.3 NATO Architecture Framework 37
2.1.4 The Open Group Architecture Framework 38

2.1.5 Zachman Framework 39
2.1.6 Academic Applications of UAF 40
2.2 Digital Engineering Foundational Literature 40
2.2.1 Department of Defense Digital Engineering Strategy 41
2.2.2 NASA Digital Engineering Implementation 42
2.2.3 INCOSE Digital Engineering Vision 43
2.2.4 Systems Engineering Body of Knowledge 44
2.3 NIST and SERC Publications 44
2.3.1 NIST Framework for Cyber-Physical Systems 44
2.3.2 NIST Systems Security Engineering Publications 45
2.3.3 NIST Digital Twin Publications 46
2.3.4 Systems Engineering Research Center Technical Reports 46
2.4 Model-Based Systems Engineering Research 47
2.4.1 Systematic Reviews of MBSE Evidence 47
2.4.2 Empirical Studies of MBSE Implementation 48
2.4.3 SysML and Modeling Language Research 48
2.4.4 The Absence of MBSE for Enterprise IT 49
2.5 Digital Twin Technology 49
2.5.1 Digital Twin Foundations 49
2.5.2 Digital Twin Standards Development 50
2.5.3 Digital Twin Security Applications 50
2.6 Barriers to Digital Engineering Adoption Beyond Defense and Aerospace . 51
2.6.1 Platform-Centric versus Enterprise Adoption Patterns 51
2.6.2 Organizational Barriers to Adoption 52
2.6.3 Technical Barriers to Adoption 53
2.6.4 Economic Barriers to Adoption 53
2.7 Open Source Standards and Tools for Digital Engineering 54

2.7.1 Open Source MBSE Tools . . . 54
2.7.2 Open Source Digital Twin Frameworks . . . 55
2.7.3 Open Source PLM Options . . . 55
2.7.4 Research Evidence for Open Source Digital Engineering Adoption . . . 56
2.8 Information Assurance and Compliance Frameworks . . . 57
2.8.1 NIST Risk Management Framework . . . 57
2.8.2 NIST SP 800-53 Security Controls . . . 57
2.8.3 CNSSI 1253 for National Security Systems . . . 58
2.8.4 ISO 27001 and Alternative Frameworks . . . 58
2.8.5 OSCAL and Automation Initiatives . . . 59
2.9 IT Service Management Literature . . . 59
2.9.1 ITIL Framework Requirements . . . 59
2.9.2 Configuration Management Database Challenges . . . 60
2.9.3 Academic Research on ITIL Implementation . . . 61
2.9.4 Shadow IT and Documentation Accuracy . . . 61
2.9.5 Change Management and Impact Assessment . . . 62
2.9.6 Integration with Information Assurance . . . 62
2.10 Enterprise Visibility and Dependency Documentation Failures . . . 62
2.10.1 Documented Scope of Visibility Failures . . . 63
2.10.2 Configuration Drift and Baseline Divergence . . . 64
2.10.3 Detection Time as Visibility Indicator . . . 64
2.10.4 Organizational Silos and Fragmented Visibility . . . 65
2.10.5 Complexity Theory Perspective . . . 66
2.10.6 Technical Debt in Documentation Domains . . . 66
2.10.7 CMDB Failure Analysis . . . 67
2.10.8 Summary of Enterprise Visibility Evidence . . . 68
2.11 Security Architecture and Threat Modeling . . . 69

2.11.1 Security Architecture Documentation Practices 70
2.11.2 Threat Modeling with MBSE 70
2.11.3 Security Control Traceability 71
2.12 Research Gaps and Theoretical Framework 71
2.12.1 Absence of Digital Engineering for Enterprise IT 71
2.12.2 Standards-Research Disconnect 72
2.12.3 Summary of Research Gaps 72
2.13 Theoretical Framework 72
2.13.1 Digital Engineering as Candidate Disciplinary Approach 73
2.13.2 Research Justification and Theoretical Contribution 75
2.13.3 Limitations of the Theoretical Framework 75
2.14 Chapter Summary 76

Chapter 3:

Research Methodology 78

3.1 Research Design Overview 78
3.1.1 Justification for Survey Methodology 79
3.1.2 Systems Engineering Approach to Research Design 82
3.1.3 Research Questions and Survey Alignment 85
3.2 Survey Requirements Specification 86
3.2.1 Anonymity and Privacy Requirements 87
3.2.2 Instrument Design Requirements 87
3.2.3 Content Requirements 88
3.3 Target Population and Sampling 89
3.3.1 Target Population 89
3.3.2 Sampling Strategy 90
3.3.3 Sample Size Determination 90
3.4 Survey Instrument Design 92

3.4.1 Instrument Overview 92
3.4.2 Question Format and Scale Selection 92
3.5 Survey Section Structure and Research Question Mapping 96
3.5.1 Section 1: Awareness and Familiarity with Digital Engineering . . . 97
3.5.2 Section 2: Understanding of Digital Engineering Capabilities 98
3.5.3 Section 3: Applicability of Digital Engineering 100
3.5.4 Section 4: Value Assessment for Information Technology 102
3.5.5 Section 5: Value Assessment for Information Assurance and Cybersecurity 104
3.5.6 Section 6: Interest and Demographic Information 106
3.5.7 Traceability of Survey Questions 108
3.6 Data Collection Procedures 108
3.6.1 Survey Platform and Administration 108
3.6.2 Data Protection Plan 109
3.6.3 Informed Consent 109
3.6.4 Recruitment and Distribution 110
3.7 Data Analysis Plan 110
3.7.1 Data Preparation and Cleaning 110
3.7.2 Descriptive Statistical Analysis 111
3.7.3 Comparative Analysis 113
3.7.4 Composite Score Analysis 114
3.7.5 Statistical Significance and Effect Sizes 115
3.7.6 Management of Type I and Type II Errors 115
3.8 Reliability and Validity Considerations 118
3.8.1 Content Validity 118
3.8.2 Construct Validity 118
3.8.3 Reliability 119

3.8.4 Pilot Testing and Instrument Refinement 119
3.8.5 Limitations 120
3.8.6 Response Bias Mitigation 122
3.9 Ethical Considerations 124
3.9.1 Anonymity 124
3.10 Research Timeline and Project Schedule 125
3.10.1 Phase 1: Committee Formation and Preparation (May 2025 – August 2025) 126
3.10.2 Phase 2: Dissertation Proposal Development (September 2025 – February 2026) 127
3.10.3 Phase 3: Proposal Defense and IRB Approval (March 2026 – April 2026) 127
3.10.4 Phase 4: Survey Execution (May 2026 – August 2026) 128
3.10.5 Phase 5: Data Analysis (September 2026 – November 2026) 128
3.10.6 Phase 6: Dissertation Writing and Defense (December 2026 – March 2027) 129
3.11 Chapter Summary 129

References 132

Appendix A: Survey Question to Research Question Mapping 145

A.1 Research Questions 145
A.2 Survey Structure Aligned to Core Dimensions 146
A.3 Section 1: Awareness and Familiarity with Digital Engineering 146
A.3.1 Rationale 148
A.4 Section 2: Understanding of Digital Engineering Capabilities 148
A.4.1 Rationale 149
A.5 Section 3: Applicability of Digital Engineering 149

A.5.1 Rationale 150
A.6 Section 4: Value Assessment for Information Technology 151
A.6.1 Rationale 151
A.7 Section 5: Value Assessment for Information Assurance 152
A.7.1 Rationale 152
A.8 Section 6: Interest and Demographic Information 153
A.8.1 Rationale 153
A.9 Summary: Question Distribution by Research Question 154
A.10 Summary: Question Distribution by DE Pillar 154
A.11 Analysis Framework 155
A.11.1 Primary Analysis for Each Research Question 155
A.11.2 Composite Scores 156
A.12 Scale Reference 156
A.12.1 Familiarity Scale (Q1.1) 156
A.12.2 Agreement Scale (Q2.1-Q5.6) 157
A.12.3 Experience Level Categories (Q6.4) 157

Appendix B: Artificial Intelligence Assistance Disclosure 158

B.1 AI Tools Utilized 158
B.2 Scope of AI Assistance 158
B.3 Scope Limitations 159
B.4 Author Responsibility 159
B.5 Rationale for Disclosure 160

LIST OF TABLES

Table 1 Revision History of the Dissertation ii

Table 2.1 Enterprise Visibility and Documentation Failure Evidence 68

Table 2.2 Research Gaps Within Corpus of Knowledge 73

Table A.1 Research Questions 145

Table A.2 Survey Section Structure 146

Table A.3 Section 1 Question Mapping 146

Table A.4 Section 2 Question Mapping 148

Table A.5 Section 3 Question Mapping 150

Table A.6 Section 4 Question Mapping 151

Table A.7 Section 5 Question Mapping 152

Table A.8 Section 6 Question Mapping 153

Table A.9 Question Distribution by Research Question 154

Table A.10 Question Distribution by Digital Engineering Pillar 154

Table A.11 Composite Score Definitions 156

Table A.12 Familiarity Scale 156

Table A.13 Agreement Scale 157

Table A.14 Experience Level Categories 157

LIST OF FIGURES

Figure 3.1 Dissertation Abstract Resource Taxonomy 84

Figure 3.2 MBSE Instantiation of Research Questions 86

Figure 3.3 Survey Question Enumeration 96

Figure 3.4 Section One Survey Question Elements Package Diagram 98

Figure 3.5 Section Two Survey Question Elements Package Diagram 100

Figure 3.6 Section Three Survey Question Elements Package Diagram 102

Figure 3.7 Section Four Survey Question Elements Package Diagram 104

Figure 3.8 Section Five Survey Question Elements Package Diagram 106

Figure 3.9 Section Six Survey Question Elements Package Diagram 107

Figure 3.10 Research Question Traceability 108

Figure 3.11 Dissertation Timeline 126

Figure A.1 Taxonomy of Survey Questions 147

Chapter 1

Introduction

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

The consequences of such failures extend beyond the immediate organizations affected. When defenders cannot comprehend the cascading impacts of compromise, risk communication to organizational leadership degrades, remediation prioritization loses connection to actual impact severity, and defensive coordination across organizational boundaries becomes impractical. The inability to understand system interdependencies transforms what might be contained incidents into enterprise-wide crises. Security teams find themselves engaged in reactive firefighting rather than proactive defense, expending resources on manual discovery efforts that 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. The term *cybersecurity* refers specifically to the technical and operational dimensions of protecting systems from cyber threats. These terms serve distinct purposes and shall not be employed interchangeably: information assurance represents the broader governance and assurance framework, while cybersecurity addresses the specific protective mechanisms and threat responses that operate within that framework.

Terminological precision bears operational consequences. Organizations that conflate information assurance with cybersecurity often underinvest in the governance, documentation, and architectural foundations upon which effective cybersecurity operations depend. The failure to maintain accurate system documentation, for example, represents an information assurance shortfall that manifests as cybersecurity operational degradation. 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. The convergence of cloud computing, microservices architectures, Internet of Things (IoT) devices, and operational technology has spawned intricate webs of interdependencies that overwhelm traditional approaches to both information assurance and IT service delivery [7]. These technological advances deliver undeniable operational benefits. But they exact a heavy toll in system visibility, security control implementation, configuration management, and service delivery coordination.

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

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

The practice of information assurance has evolved in response to the complexities of modern enterprise environments. The NIST Risk Management Framework provides a structured, disciplined approach for managing security and privacy risk that organizations can apply across diverse information systems [4]. The RMF establishes a lifecycle approach to security through seven iterative steps: prepare, categorize, select, implement, assess, authorize, and monitor. This framework has become foundational for federal agencies and finds increasing adoption among organizations operating national security systems and private enterprises seeking systematic approaches to information assurance.

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

Additional information assurance lifecycle frameworks exist including ISO 31000 [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.

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

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

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

1.1.2 IT Service Management Practice

IT service management (ITSM) has matured through frameworks designed to ensure reliable service delivery across the enterprise. The Information Technology Infrastructure Library provides comprehensive guidance for aligning IT services with business needs through structured processes for service strategy, service design, service transition, service operation, and continual service improvement [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. The challenge lies in the mismatch between the documentation velocity that manual processes can sustain and the operational velocity that modern enterprise environments demand. No amount of process improvement or additional staffing can close this gap using traditional approaches. The solution requires a paradigm shift from document-centric to model-centric practices—precisely the shift that Digital Engineering provides.

Research documents pervasive failures across both information assurance and IT service management domains. Industry analysts report that eighty percent of Configuration Management Database (CMDB) implementations fail to deliver intended value [13]. Studies find that organizations can monitor only sixty-six percent of their IT environments, leaving thirty-four percent unmonitored [14]. 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 [15]. The mean time to identify security breaches averages 204 days, reflecting the visibility gaps that impair threat detection [16].

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

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

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

1.2 Digital Engineering as Potential Solution

Digital Engineering represents a systematic approach to designing, developing, and managing complex systems through integrated digital models and data-driven processes [17]. Originally forged within the defense and aerospace sectors, Digital Engineering has been formalized through authoritative guidance from organizations including the United States Department of Defense (DoD) [18], the National Aeronautics and Space Administration (NASA) [19], and the International Council on Systems Engineering (INCOSE) [17]. While these foundational practices emerged primarily from physical systems engineering, the underlying principles offer capabilities of documented value for information technology and information assurance domains.

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

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

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

1.2.1 Model-Based Systems Engineering

Model-Based Systems Engineering represents a paradigm shift from document-centric practices to model-centric approaches for system development and management [20]. 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 [21].

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

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

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

1.2.2 Digital Threads

Digital threads constitute authoritative traceability—the verified, bidirectional connections between requirements, design elements, implementation artifacts, and validation activities that persist throughout a system's lifecycle [22]. The term "digital threads" describes the connective tissue that weaves together authoritative sources including Model-Based Systems Engineering models, requirements management systems, configuration management databases, and Product Lifecycle Management repositories into a unified, navigable fabric of system information. Digital threads ensure that organizations can track how requirements flow through the development and implementation process, identify which system components implement specific capabilities, and verify that implemented solutions satisfy intended requirements. Unlike traditional documentation approaches, digital threads maintain verified relationships that remain current as systems evolve [23].

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

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

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

1.2.3 Digital Twin

Digital twin technology creates virtual replicas of physical or logical systems that maintain synchronization with their real-world counterparts through continuous data exchange [24]. These virtual representations enable organizations to simulate system behavior, analyze potential changes, predict future states, and optimize performance without disrupting operational systems [25]. Digital twins combine real-time operational data with analytical models to provide dynamic, predictive capabilities that extend far beyond traditional monitoring and simulation approaches [26].

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

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

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

1.2.4 Product Lifecycle Management

Product Lifecycle Management provides frameworks and toolsets for managing information, processes, and resources throughout a system's entire lifecycle from initial conception through retirement [27]. PLM integrates data from diverse sources, maintains configuration baselines, manages change processes, and ensures that stakeholders access current, accurate information about system states and changes. This integrated approach to lifecycle management extends beyond simple version control to encompass configuration management, change coordination, release management, and information governance.

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

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

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

1.3 Gaps in Current Practice

Despite advances in information assurance methodologies and IT service management frameworks, organizations continue to encounter challenges that limit their effectiveness in protecting information assets and delivering reliable services. The NIST Risk Management Framework and ITIL provide structured approaches to information assurance and IT service management respectively. Yet implementation challenges persist across both domains. 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. This visibility gap manifests throughout the RMF lifecycle: organizations find it difficult to track security dependencies effectively, leading to unidentified vulnerabilities when changes are implemented. The inability to maintain accurate documentation of system interconnections and data flows, particularly in environments with rapid deployment cycles, impairs the effective risk assessment and incident response capabilities that the RMF demands.

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

Security control implementation presents particular challenges in modern enterprise environments characterized by hybrid cloud deployments, distributed architectures, and frequent changes. Organizations must implement and maintain consistent security controls from NIST SP 800-53 across diverse platforms while supporting continuous deployment practices and rapid update cycles [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 [13]. 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 infrastructure. IT teams cannot effectively manage changes without understanding security implications. Both domains require the visibility and accurate documentation that current practices demonstrably fail to provide.

1.3.3 The Documentation-Reality Gap

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

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

Digital Engineering 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.

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

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

1.5.1 Methodological Approach

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

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

1.5.2 Target Population and Broader Application

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

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

The defense and aerospace sectors have demonstrated measurable benefits from Digital Engineering adoption. The Department of Defense Digital Engineering Strategy documents improved mission assurance, reduced development timelines, and enhanced configuration management across programs implementing Digital Engineering practices [3]. NASA reports similar benefits from Model-Based Systems Engineering adoption across its mission portfolio [28]. These demonstrated benefits establish that Digital Engineering delivers value in complex, mission-critical contexts requiring stringent compliance and comprehensive documentation.

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

1.5.3 Potential Benefits for Organizations Serving Underrepresented Populations

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

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

If Digital Engineering practices can reduce the burden of compliance documentation while improving documentation accuracy, organizations with limited resources could redirect staff effort toward direct service provision rather than documentation administration.

The automated traceability that digital threads provide could reduce the manual effort required for compliance audits. The model-based documentation that MBSE enables could maintain accuracy through automated synchronization rather than manual updates. The configuration management capabilities that PLM provides could reduce the specialized expertise required to maintain accurate system documentation.

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

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

1.5.4 Why Perceptions Matter

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

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

1.5.5 Contribution of Prior Research

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

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

1.6 Significance of the Research

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

1.6.1 Academic Significance

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

This research contributes empirical evidence to a domain currently characterized by theoretical proposition rather than data. The 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.

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

1.6.3 Commonwealth Significance

The commonwealth significance of this research relates to national security and protection of societal infrastructure. Federal information systems and national security systems protect information assets and enable government operations upon which citizens depend. Organizations operating these systems face the challenges documented throughout this proposal: maintaining accurate documentation, implementing consistent security controls, and verifying compliance across complex technical environments.

Digital threads, 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

This chapter has established the context for investigating professional awareness and perceptions of Digital Engineering capabilities within information assurance and IT service management domains. The discussion identified the challenges organizations face in maintaining accurate system documentation, implementing consistent security controls, and delivering reliable IT services using traditional document-centric approaches. Digital

Engineering, with its four pillars of Model-Based Systems Engineering, digital threads, digital twin technology, and Product Lifecycle Management, offers capabilities that have demonstrated value in defense and aerospace contexts and that may address analogous gaps in enterprise IT and information assurance practice.

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

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

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

Chapter 2

Literature Review

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

2.1 Enterprise Architecture Frameworks

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

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

2.1.1 The Unified Architecture Framework

The Unified Architecture Framework represents the most notable evolution in enterprise architecture standardization, now codified as ISO/IEC 19540-1:2022 and ISO/IEC 19540-2:2022 through the Object Management Group [6]. UAF emerged from the Unified Profile for DoDAF and the Ministry of Defence Architecture Framework (MODAF) (UPDM 3.0) with the explicit purpose of consolidating multiple defense architecture frameworks while extending applicability to commercial domains. The specification asserts that ninety percent of concepts and themes captured in military frameworks prove equally applicable in commercial domains [30]. This recognition carries implications for enterprise IT and Information Assurance practitioners who have historically operated outside the systems engineering discipline.

UAF employs a grid-based structure wherein rows represent stakeholder domains—Strategic, Operational, Services, Personnel, and Resources—while columns represent architecture aspects. This structure defines seventy-one view specifications through the

UAF Domain Metamodel and UAF Modeling Language [31]. The framework's foundation upon the IDEAS Ontology and implementation through UML/SysML profiles addresses a historical limitation: the disconnect between enterprise architecture and systems engineering tools that plagued earlier frameworks [32]. For organizations seeking to bridge the gap between enterprise IT documentation and rigorous systems engineering practice, UAF provides a standards-based pathway.

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

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

2.1.1.1 UAF as the Consolidating Standard

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

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

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

The Department of Defense has incorporated UAF into its architecture guidance, recognizing the framework's alignment with Digital Engineering initiatives [18]. The UK Ministry of Defence maintains alignment between MODAF evolution and UAF development. NATO Architecture Framework Version 4 explicitly endorses the UAF Domain Metamodel as a compliant metamodel, validating UAF's role as a unifying framework for defense interoperability across allied nations [36]. This adoption by major defense organizations establishes UAF as the authoritative approach for defense architecture while the ISO standardization extends that authority to commercial contexts.

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

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

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

2.1.2 Department of Defense Architecture Framework

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

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

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

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

2.1.3 NATO Architecture Framework

The NATO Architecture Framework (NAF) Version 4 explicitly endorses the UAF Domain Metamodel as a compliant metamodel, validating UAF's role as a unifying framework for defense interoperability across allied nations [36]. NAF evolved through multiple versions to address interoperability requirements spanning NATO member nations, with Version 4 representing alignment with international standardization efforts. The framework supports coalition operations planning and capability development through standardized architectural descriptions that enable communication across organizational and national boundaries.

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

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

2.1.4 The Open Group Architecture Framework

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

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

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

2.1.5 Zachman Framework

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

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

2.1.6 Academic Applications of UAF

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

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

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

2.2 Digital Engineering Foundational Literature

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

2.2.1 Department of Defense Digital Engineering Strategy

The Department of Defense Digital Engineering Strategy, published in June 2018, established the formal vision for transforming defense acquisition through Digital Engineering practices [3]. The strategy defines five strategic goals: formalize the development, integration, and use of models to inform enterprise and program decisions; provide an authoritative source of truth; incorporate technological innovation to improve engineering practice; establish a Digital Engineering ecosystem; and transform the culture and workforce to adopt Digital Engineering.

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

The authoritative source of truth concept deserves particular attention because it directly addresses the documentation-reality gap identified in Chapter 1. The DoD strategy defines the authoritative source of truth as “a single source of data and models” that provides “a definitive technical baseline” for programs [3]. This concept recognizes that multiple documentation sources inevitably diverge, creating the ambiguity and inconsistency that undermine both engineering decisions and compliance verification. Digital Engineering addresses this challenge by establishing single authoritative sources from which all views, reports, and analyses are generated.

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

The Systems Engineering Guidebook, published by the Office of the Under Secretary of Defense for Research and Engineering in February 2022, provides detailed implementation guidance for Digital Engineering practices within defense programs [18]. The guidebook addresses model-based systems engineering, digital thread implementation, digital twin employment, and the integration of these capabilities within program management and acquisition processes.

2.2.2 NASA Digital Engineering Implementation

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

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

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

2.2.3 INCOSE Digital Engineering Vision

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

The INCOSE Systems Engineering Handbook, Fifth Edition, published in 2023, elaborates upon ISO/IEC/IEEE 15288:2023 life cycle processes with specific MBSE methodology guidance [51]. The handbook provides the authoritative reference for systems engineering practice, integrating Digital Engineering concepts throughout. The INCOSE Digital Engineering Information Exchange Working Group promotes collaboration and knowledge sharing among practitioners implementing Digital Engineering practices [17].

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

2.2.4 Systems Engineering Body of Knowledge

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

2.3 NIST and SERC Publications

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

2.3.1 NIST Framework for Cyber-Physical Systems

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

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

2.3.2 NIST Systems Security Engineering Publications

NIST's systems security engineering publications establish principles for engineering trustworthy secure systems. Special Publication 800-160 Volume 1 Revision 1 describes a basis for establishing principles, concepts, activities, and tasks for engineering systems that merit stakeholder trust [27]. Special Publication 800-160 Volume 2 Revision 1 complements Volume 1 by addressing cyber resiliency considerations [54].

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

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

2.3.3 NIST Digital Twin Publications

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

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

2.3.4 Systems Engineering Research Center Technical Reports

The Digital Engineering Competency Framework, documented in technical report SERC-2021-TR-005, defines 962 Knowledge, Skills, Abilities, and Behaviors organized by proficiency levels [21]. The Digital Engineering Metrics technical report, SERC-2020-TR-002, develops frameworks for measuring Digital Engineering benefits and adoption [20]. Additional SERC technical reports address enterprise system-of-systems modeling and systems engineering modernization [57], [58].

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

2.4 Model-Based Systems Engineering Research

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

2.4.1 Systematic Reviews of MBSE Evidence

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

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

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

2.4.2 Empirical Studies of MBSE Implementation

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

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

2.4.3 SysML and Modeling Language Research

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

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

2.4.4 The Absence of MBSE for Enterprise IT

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

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

2.5 Digital Twin Technology

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

2.5.1 Digital Twin Foundations

Grieves traces the evolution of digital twin concepts from Product Lifecycle Management origins through contemporary applications [65]. Grieves, who originated the digital twin concept, positions it as the integration of physical and virtual systems that enables analysis, optimization, and prediction. Research by Madni and Sievers provides a framework for leveraging digital twins in systems engineering contexts [25]. Khan et al. examine digital twin applications in emerging technology contexts [26].

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

2.5.2 Digital Twin Standards Development

Shao examines ISO 23247 and IEC 62832 standards for digital twin frameworks [24]. Shao et al. provides additional analysis of ISO 23247's four-part structure [56]. These standards establish interoperability requirements for digital twin implementations, addressing data exchange, interface specifications, and functional requirements.

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

2.5.3 Digital Twin Security Applications

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

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

2.6 Barriers to Digital Engineering Adoption Beyond Defense and Aerospace

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

2.6.1 Platform-Centric versus Enterprise Adoption Patterns

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

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

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

2.6.2 Organizational Barriers to Adoption

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

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

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

2.6.3 Technical Barriers to Adoption

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

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

2.6.4 Economic Barriers to Adoption

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

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

2.7 Open Source Standards and Tools for Digital Engineering

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

2.7.1 Open Source MBSE Tools

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

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

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

2.7.2 Open Source Digital Twin Frameworks

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

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

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

2.7.3 Open Source PLM Options

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

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

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

2.7.4 Research Evidence for Open Source Digital Engineering Adoption

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

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

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

2.8 Information Assurance and Compliance Frameworks

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

2.8.1 NIST Risk Management Framework

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

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

2.8.2 NIST SP 800-53 Security Controls

NIST Special Publication 800-53 Revision 5 provides the security control catalog for federal information systems [4]. Multiple controls explicitly require enterprise architecture capabilities: PL-2 requires security plans consistent with enterprise architecture; PL-8 requires security architecture development; PM-7 establishes enterprise architecture requirements; CM-2 requires documented baselines; CM-8 requires accurate system component inventory; SA-17 requires design specifications consistent with enterprise architecture.

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

2.8.3 CNSSI 1253 for National Security Systems

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

2.8.4 ISO 27001 and Alternative Frameworks

Organizations outside federal requirements may employ alternative security control frameworks. ISO/IEC 27001:2022 provides an international standard for information security management systems [12]. These alternative frameworks share common characteristics with NIST guidance: they assume documentation accuracy and visibility capabilities that organizations struggle to maintain. Digital Engineering could address documentation requirements across frameworks regardless of which specific framework organizations employ.

2.8.5 OSCAL and Automation Initiatives

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

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

2.9 IT Service Management Literature

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

2.9.1 ITIL Framework Requirements

The Information Technology Infrastructure Library provides guidance for IT service management [5]. ITIL 4 reorganized service management practices and introduced the Service Value System concept [84]. Despite recognizing that tracking configurations across virtual systems, cloud computing, and cybersecurity domains presents challenges, ITIL provides limited guidance on addressing documentation accuracy challenges.

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

2.9.2 Configuration Management Database Challenges

Configuration Management Database implementation failures stand extensively documented in industry research. Gartner reports an eighty percent failure rate for CMDB implementations [13]. Additional research indicates that ninety-nine percent of organizations using CMDB tooling without addressing data quality gaps will experience visible business disruption [85]. Forrester research finds that less than half of organizations trust the data in their CMDB [86].

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

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

2.9.3 Academic Research on ITIL Implementation

Cook et al. found resistance to change at twenty-seven percent as the top ITIL implementation challenge [89]. Marrone and Kolbe surveyed 491 firms finding that while over ninety percent use ITSM frameworks, little research examines actual benefits realized [90]. Research by Benbya et al. demonstrates that enterprise information systems have reached complexity levels exceeding prior technological generations [7].

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

2.9.4 Shadow IT and Documentation Accuracy

Gartner research indicates forty-one percent of employees used shadow IT in 2022, expected to climb to seventy-five percent by 2027 [15]. Thirty to forty percent of large companies' IT expenditure represents shadow IT. Shadow IT undermines configuration management because systems deployed without IT oversight cannot be documented. No manual process can maintain awareness of systems that bypass official acquisition and deployment channels.

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

2.9.5 Change Management and Impact Assessment

Industry analysis confirms that reliance upon outdated documentation leads to inaccurate impact assessments [91]. Research by Bokan and Santos highlights difficulties organizations encounter in maintaining comprehensive security oversight [8]. Change management depends upon accurate understanding of system relationships [92] that current documentation approaches cannot maintain.

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

2.9.6 Integration with Information Assurance

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

2.10 Enterprise Visibility and Dependency Documentation Failures

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

2.10.1 Documented Scope of Visibility Failures

Research consistently documents that organizations lack visibility into large portions of their IT environments. IDC and Exabeam found that organizations globally can monitor only sixty-six percent of their IT environments, leaving blind spots particularly in cloud deployments [14]. The Ponemon Institute's 2023 Global Study on Closing the IT Security Gap found that sixty-three percent of security teams lack visibility and control into all user device activity connected to their infrastructure [94]. The SANS Institute SOC Survey found that only fifteen percent of respondents expressed very high confidence that all devices on their network are discoverable [95].

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

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

2.10.2 Configuration Drift and Baseline Divergence

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

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

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

2.10.3 Detection Time as Visibility Indicator

Breach detection times serve as proxy measures for organizational visibility into their information systems. IBM Security and Ponemon Institute report that the mean time to identify breaches reached two hundred four days, with breaches involving lifecycles exceeding two hundred days costing an average of 5.46 million dollars [16]. The 2024 report found that only forty-two percent of breaches were detected internally. Stolen credential breaches—reflecting authentication and identity management documentation failures—required two hundred ninety-two days to identify and contain, the longest of any attack vector.

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

2.10.4 Organizational Silos and Fragmented Visibility

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

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

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

2.10.5 Complexity Theory Perspective

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

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

2.10.6 Technical Debt in Documentation Domains

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

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

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

2.10.7 CMDB Failure Analysis

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

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

2.10.8 Summary of Enterprise Visibility Evidence

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

Table 2.1: Enterprise Visibility and Documentation Failure Evidence

Finding	**Statistic**	**Source**
	Visibility Gap Metrics	
IT environment monitorable	66%	IDC/Exabeam 2023[14]
Security teams lacking device visibility	63%	Ponemon Institute 2023[94]
High confidence in device discovery	15%	SANS Institute 2023[95]
Organizations with security/IT silos	55%	Ivanti 2025[96]
	Configuration Management Failures	
CMDB implementation failure rate	80%	Gartner Research[13], [85]
Outages from configuration issues	64%	Uptime Institute 2023[102]
Misconfigurations from parameter errors	70-85%	Yin et al. 2011[100]
Unplanned outages from ill-planned changes	80%	IT Process Institute[103]
	Shadow IT and Undocumented Assets	
Shadow IT as percentage of IT spend	30-40%	Gartner Research[15]
Cloud services vs. IT estimates	15-22x higher	Cisco 2016[113]
Employees using shadow IT (2022)	41%	Gartner Research[15]
Projected shadow IT usage (2027)	75%	Gartner Research[15]
	Security Impact Metrics	
Mean time to identify breach	204 days	IBM/Ponemon 2024[16]
Cloud breaches from misconfigurations	82%	Check Point 2024[98]
Organizations with cloud breaches (18 mo)	95%	CSA 2024[97]
Projected preventable cloud breaches (2027)	99%	Gartner Research[114]

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

A methodological observation regarding the evidentiary sources presented in this section warrants acknowledgment. The enterprise visibility evidence draws substantially upon industry analyst reports and practitioner surveys alongside peer-reviewed academic research. This 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. The 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, Santos et al. on documentation technical debt, and Li et al. on technical debt taxonomies—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.

2.11 Security Architecture and Threat Modeling

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

2.11.1 Security Architecture Documentation Practices

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

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

2.11.2 Threat Modeling with MBSE

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

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

2.11.3 Security Control Traceability

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

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

2.12 Research Gaps and Theoretical Framework

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

2.12.1 Absence of Digital Engineering for Enterprise IT

The academic research gap is pronounced. Systematic literature reviews examining MBSE consistently find no research addressing enterprise IT infrastructure or Information Assurance applications beyond the preliminary reference model by Bonar and Hastings [29], discussed in Section 2.7. This gap persists despite explicit requirements in compliance frameworks for capabilities that Digital Engineering provides.

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

2.12.2 Standards-Research Disconnect

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

2.12.3 Summary of Research Gaps

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

2.13 Theoretical Framework

Based upon the systematic literature review, this research adopts a theoretical framework integrating Digital Engineering principles with established Information Assurance and IT Service Management practices. This framework posits that Digital Engineering represents a disciplinary approach with demonstrated value in defense and aerospace contexts whose capabilities align with gaps that have persisted in enterprise IT despite decades of framework development and organizational investment. The framework does

Table 2.2: Research Gaps Within Corpus of Knowledge

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

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 DE capabilities and documented enterprise IT challenges, establishing the theoretical basis for investigating whether practitioners recognize these correspondences.

2.13.1 Digital Engineering as Candidate Disciplinary Approach

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.

2.13.1.1 Addressing the Authoritative Source of Truth Gap

The DoD Digital Engineering Strategy defines the authoritative source of truth as a single source of data and models providing a definitive technical baseline [3]. Current IT and Information Assurance practices lack authoritative sources of truth, instead maintaining multiple disconnected documentation artifacts that diverge over time. Digital Engineering's emphasis upon authoritative sources addresses this gap by establishing single, model-based repositories from which all views and reports are generated.

2.13.1.2 Addressing the Traceability Gap

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

2.13.1.3 Addressing the Visibility Gap

Visibility into system configurations, dependencies, and states represents a core requirement for both IT Service Management and Information Assurance. Current practices fail to provide this visibility, with research documenting eighty percent CMDB failure rates and pervasive shadow IT [13], [15]. Model-based approaches that maintain synchronization with operational systems address this gap by providing visibility that manual documentation cannot sustain.

2.13.1.4 Addressing the Simulation and Testing Gap

Digital twin capabilities enable organizations to simulate system behavior, test proposed changes, and analyze scenarios without affecting production systems. Current IT Service

Management practices lack simulation capabilities for change impact analysis. Current Information Assurance practices lack simulation capabilities for security control validation. Digital twins address these gaps by providing virtual environments synchronized with operational systems for testing and analysis.

2.13.2 Research Justification and Theoretical Contribution

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

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

2.13.3 Limitations of the Theoretical Framework

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

2.14 Chapter Summary

This literature review has examined the current body of knowledge across nine interconnected domains relevant to applying Digital Engineering methodologies to Information Assurance and IT Service Management. The review established that Digital Engineering has demonstrated value in aerospace, defense, and manufacturing contexts, with authoritative guidance from organizations including the Department of Defense, NASA, and INCOSE providing mature frameworks and methodologies. Yet systematic examination across major academic databases revealed a pronounced research gap: apart from the preliminary reference model by Bonar and Hastings [29], no peer-reviewed research addresses Digital Engineering application to enterprise IT infrastructure, IT Service Management, or Information Assurance programs.

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

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

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

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

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. The study deploys a quantitative survey-based approach to collect data from IT and information assurance professionals, enabling systematic analysis of awareness levels, perceived value, and anticipated benefits of Digital Engineering practices for information assurance and IT service delivery. The methodology itself follows a systems engineering lifecycle approach—demonstrating 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. This research selected survey methodology 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. Additionally, 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

The question of whether perceived value merits dissertation-level investigation reflects a particular view of research contribution. This research contributes to knowledge by addressing a documented gap: the academic literature contains no investigation of whether IT and Information Assurance professionals perceive value in Digital Engineering capabilities. The theoretical framework presented in Chapter 2 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 applicability 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.

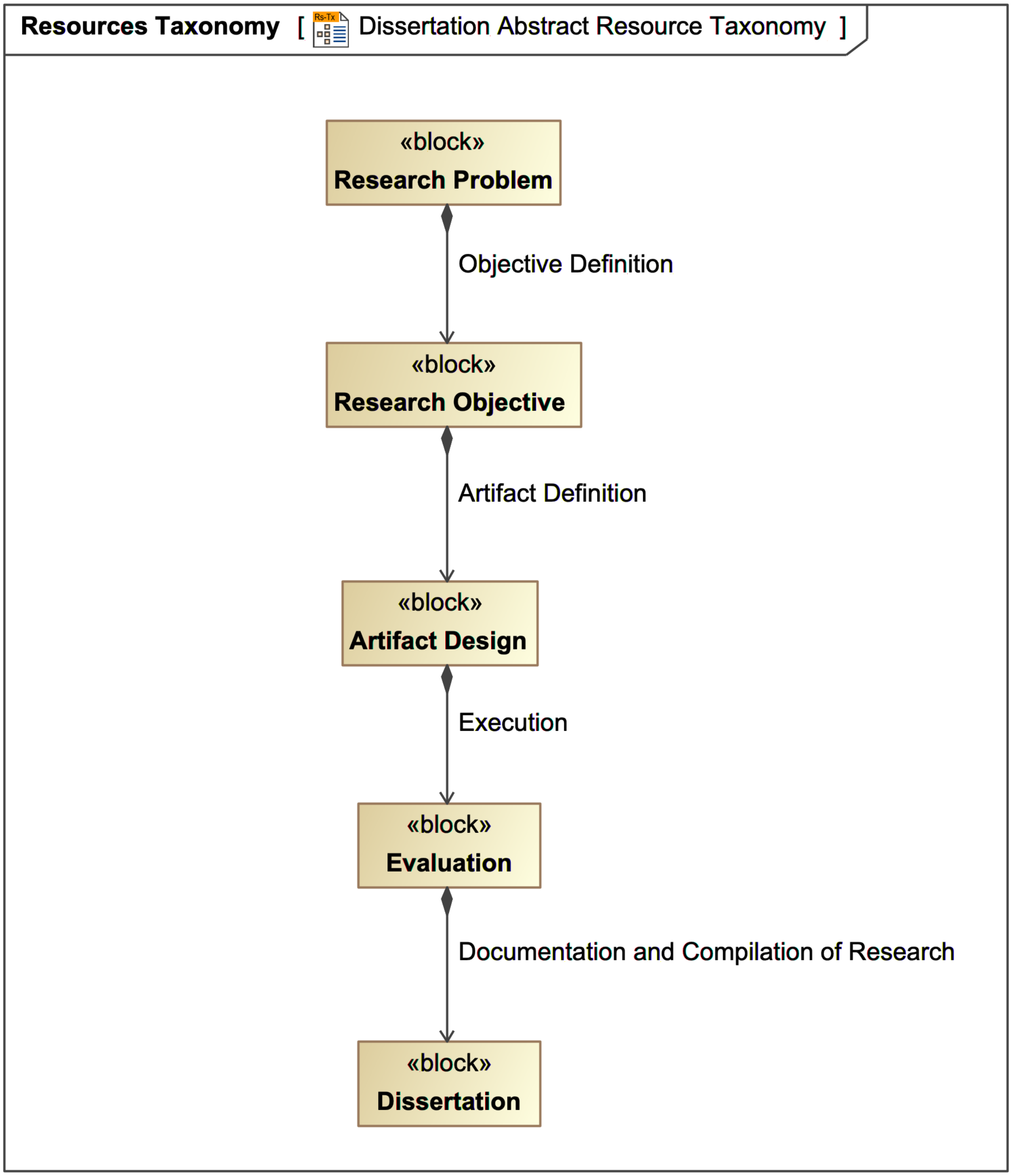
3.1.2.6 Report Phase

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. The selection of requirement type element within the UAF allows for survey questions to utilize "Satisfy" relationship. The use of authoritative traceability within the model enables programatic evaluation of the model and simulation to validate the model.

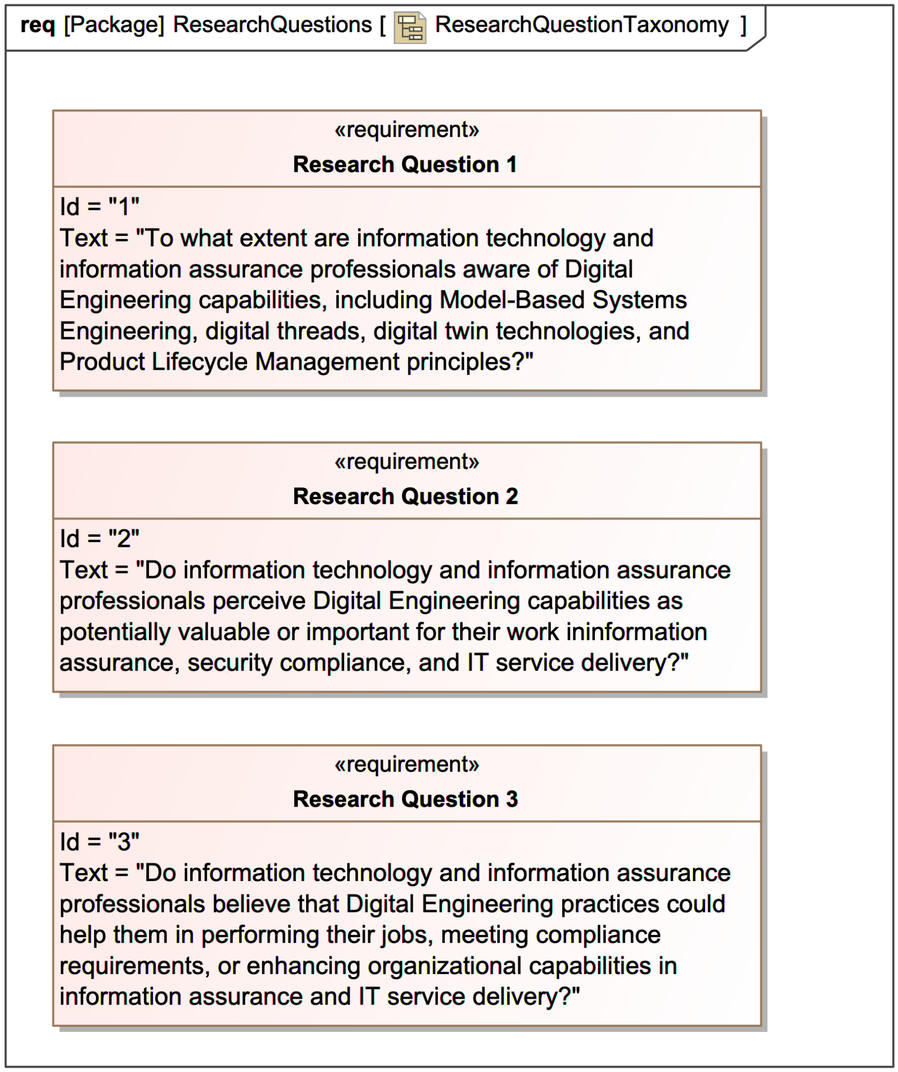


Figure 3.2: MBSE Instantiation of Research Questions

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

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

The 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"). This framing reflects a deliberate design decision informed by the research objectives and target population characteristics. 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. The neutral midpoint ("Neither agree nor disagree") provides a non-affirmative response option for respondents who are genuinely uncertain or indifferent. 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

The target population for this study consists of professionals actively working in information technology and information assurance roles within organizations that manage information systems. This population encompasses 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, $(\mathrm{ISC})^2$, 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 [117]. 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 [118]. 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

The survey instrument consists of 27 questions organized into six thematic sections designed to systematically address the research questions while maintaining reasonable completion time. The 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

The survey employs two primary question formats: five-point Likert-type scales and binary (yes/no) response options. The 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 [119] argues that Likert data are strictly ordinal and that parametric analyses may produce misleading results. Norman [120], 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 [121] and de Winter and Dodou [122] 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.

The consistent use of Likert scales across sections provides an intuitive response method for participants and enables direct comparison of responses across different constructs. The scales employed in this survey use two distinct anchor sets 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

The agreement scale follows established conventions in technology acceptance research, including the Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) frameworks, which have demonstrated validity for measuring perceptions of technology value and usefulness across diverse populations and contexts. The inclusion of 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.

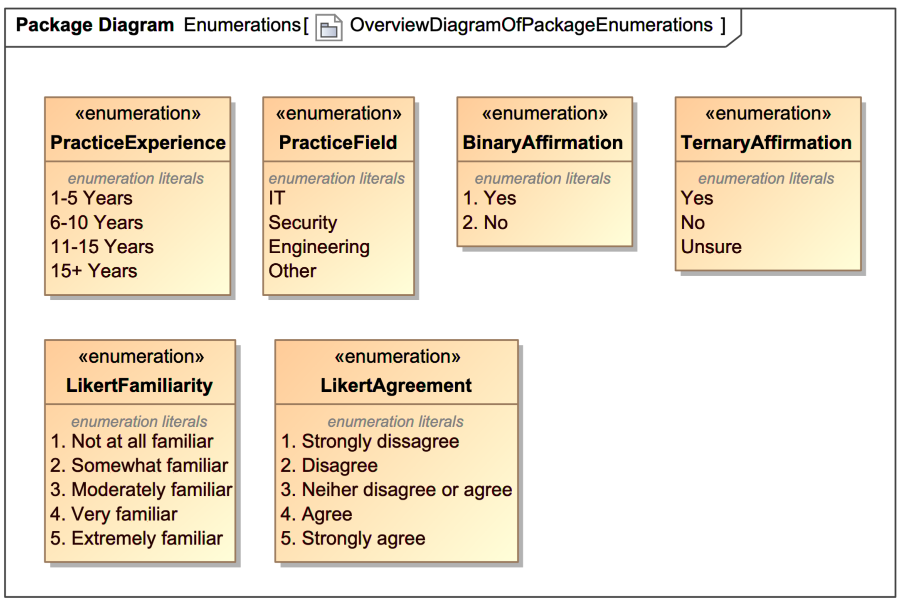


Figure 3.3: Survey Question Enumeration

3.5 Survey Section Structure and Research Question Mapping

This section details how each survey section addresses the research questions, providing explicit traceability between survey content and research objectives. This mapping ensures that every question serves a defined purpose and 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 3.4 provides an MBSE based visualization as a block element.

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.

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.

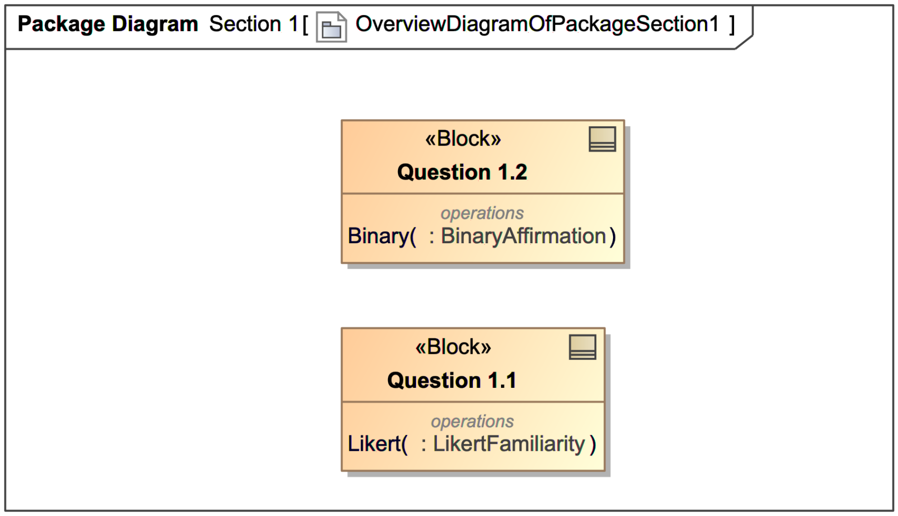


Figure 3.4: Section One Survey Question Elements Package Diagram

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 3.5 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."

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

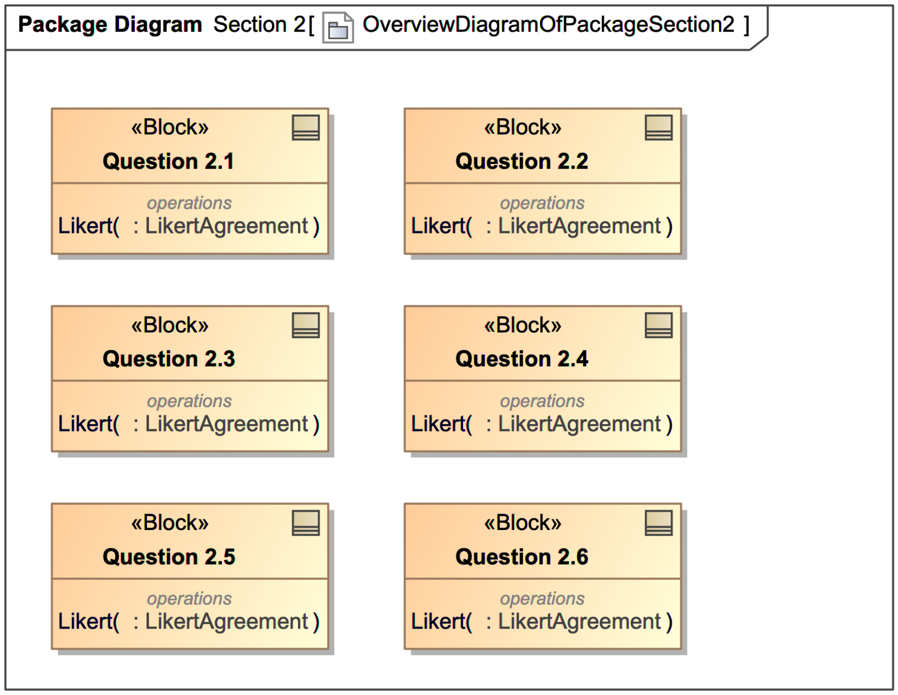


Figure 3.5: Section Two Survey Question Elements Package Diagram

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 3.6.

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."

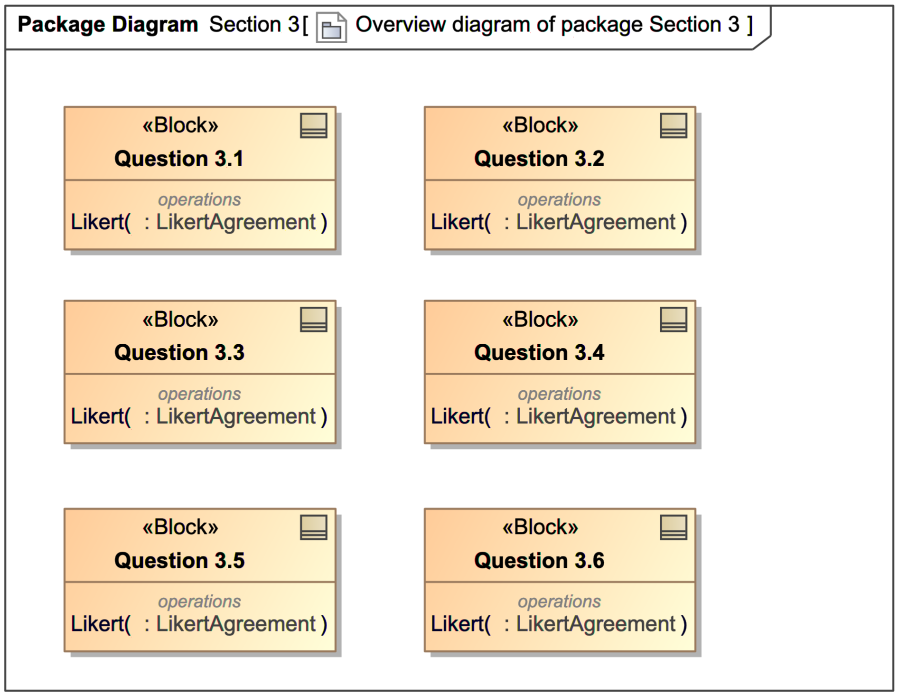


Figure 3.6: Section Three Survey Question Elements Package Diagram

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 3.7

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)

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.

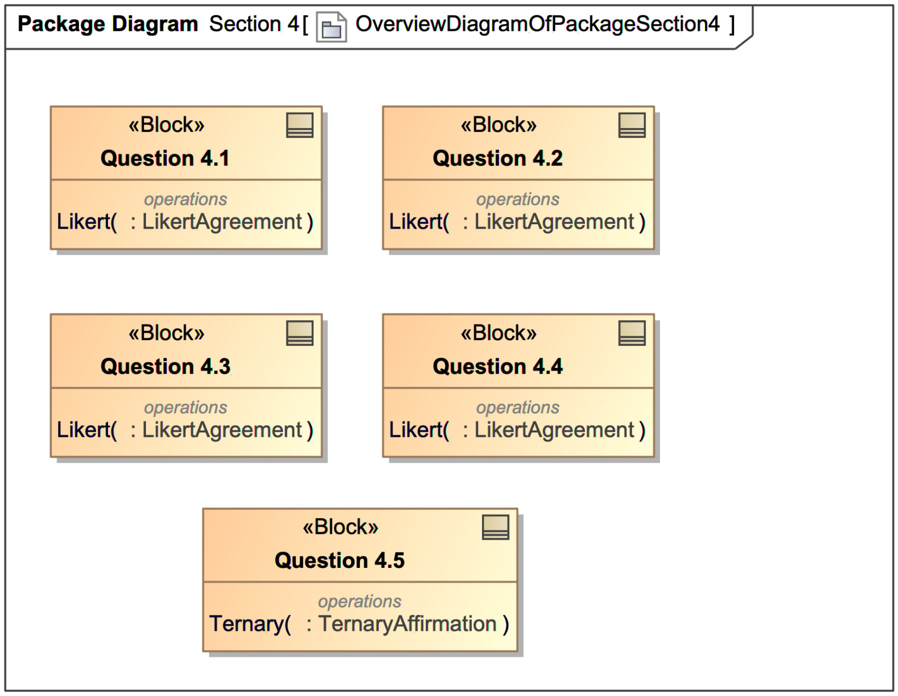


Figure 3.7: Section Four Survey Question Elements Package Diagram

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 3.8.

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)

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.

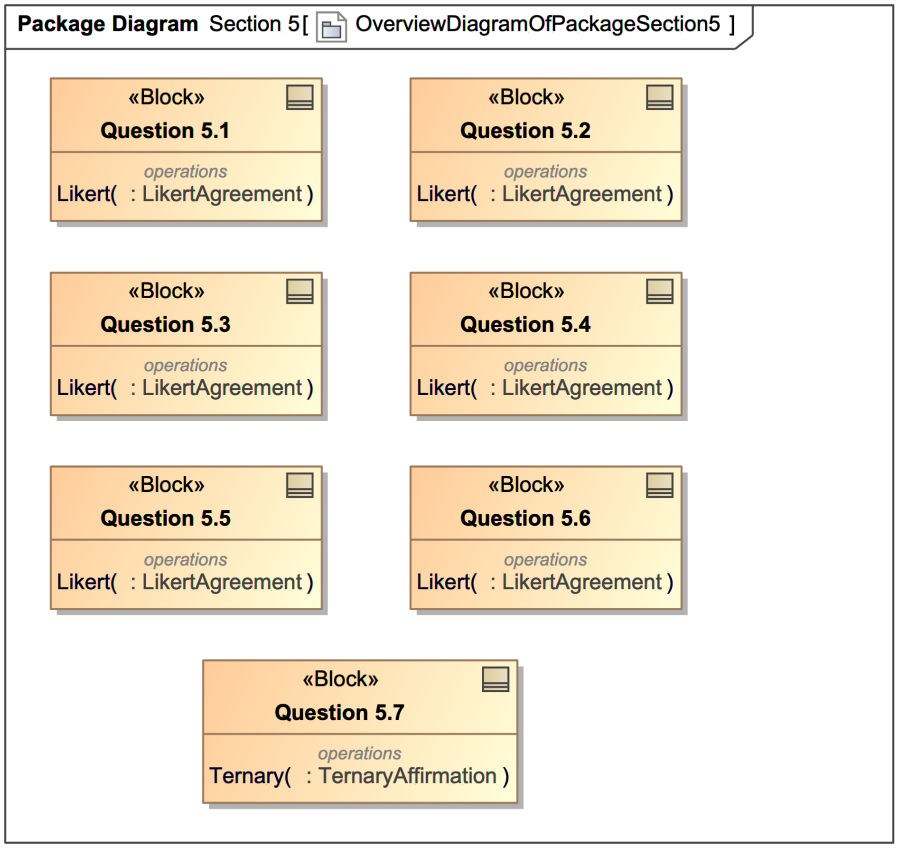


Figure 3.8: Section Five Survey Question Elements Package Diagram

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 3.9 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

This question captures professional field: "Please indicate your field of practice." (Information Technology / Security / Engineering / Other). The use of "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. The 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)

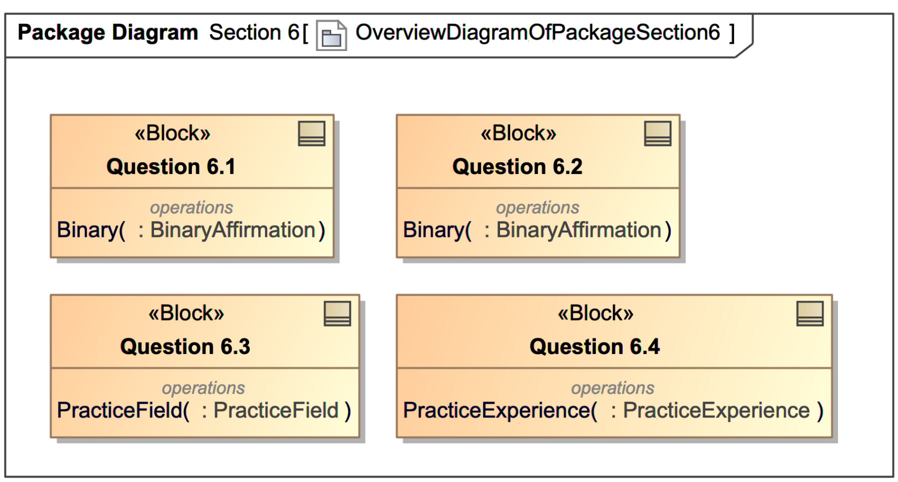


Figure 3.9: Section Six Survey Question Elements Package Diagram

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 3.10 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.

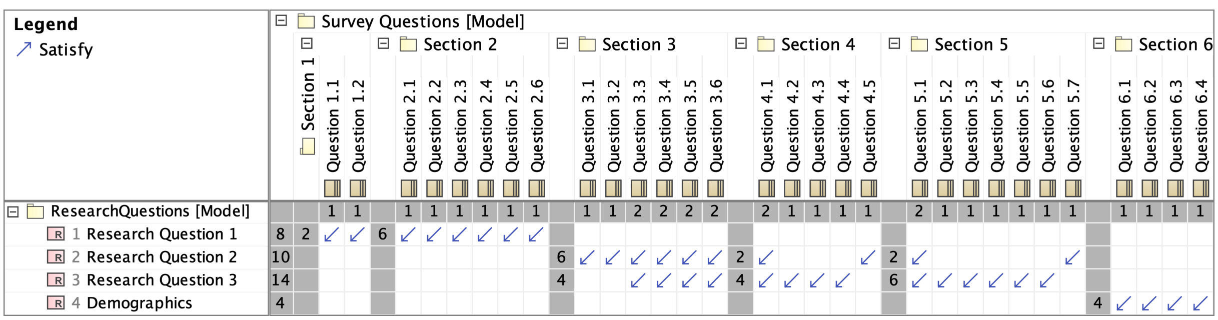


Figure 3.10: Research Question Traceability

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

The survey begins with a comprehensive participation notice explaining the research purpose, what participation involves, confidentiality protections, voluntary nature of participation, and contact information for questions or concerns. The notice clearly 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 $\geq$ 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

The analytical design incorporates multiple provisions to 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). These provisions operate at the levels of sample design, instrument design, and analytical procedure.

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

The survey instrument design contributes to error management through several structural features. The use of established five-point Likert scales with validated anchor sets reduces 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. The agreement scale format follows conventions from TAM and UTAUT research that have demonstrated validity for measuring technology perceptions across diverse populations. The tripartite structure of the survey 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

The survey instrument underwent pilot testing during the Spring 2024 semester prior to formal dissertation proposal development. The pilot study administered an earlier version of the instrument 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 requiring 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 genuinely 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.

The survey questions in Sections 2 through 5 incorporate minimal contextual descriptions of Digital Engineering capabilities within the question stems. This design choice reflects a deliberate balance between two competing methodological concerns. 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 empirical 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. The timeline aligns with Dakota State University's doctoral program requirements and academic calendar while accommodating 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 3.11 presents the project schedule as a gantt chart.

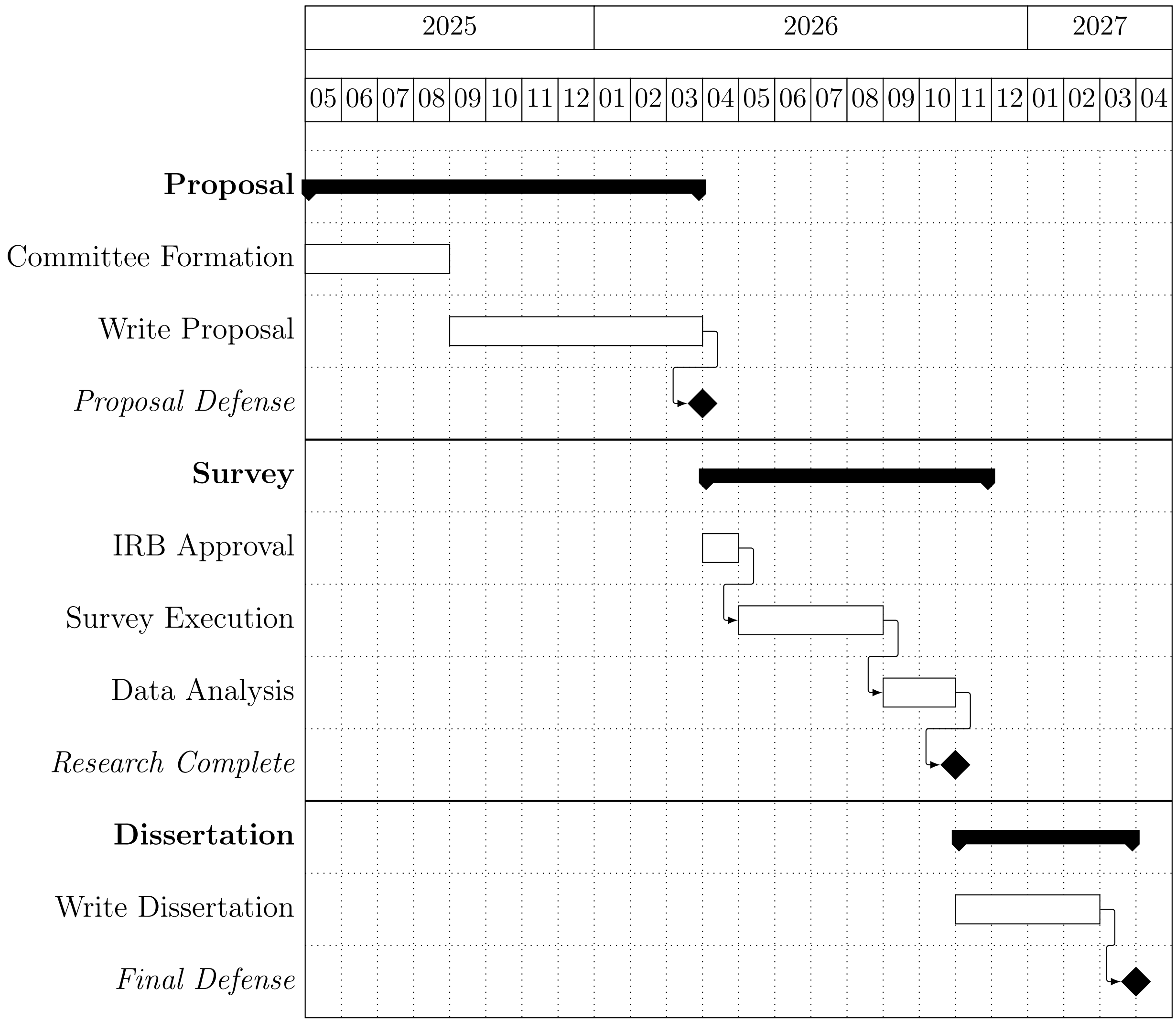


Figure 3.11: Dissertation Timeline

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 members addressed research scope, methodology, and expected timeline. Committee formation concluded in January 2026, 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 drafts 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)

The dissertation proposal defense occurs in March 2026, providing the committee opportunity to evaluate the research design before data collection commences. The defense presentation addresses the research problem, theoretical framework, methodology, and anticipated contributions. 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. The IRB application includes the complete research protocol, survey instrument, recruitment materials, informed consent procedures, and data protection plan. The timeline allocates April 2026 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.

The dissertation final defense occurs in March 2027, approximately twenty-two months after the research project commenced. The defense presentation summarizes the complete research project, emphasizing 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. The research employs a quantitative survey methodology following a systems engineering lifecycle approach that ensures rigor and traceability throughout the research process. The survey instrument, refined through pilot testing conducted during the Spring 2024 semester, 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.

The methodology incorporates proactive response bias mitigation 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. These provisions complement the acknowledged limitations of non-probability sampling and self-selection to strengthen confidence in the validity of collected data.

The methodology establishes a rigorous foundation for generating empirical evidence regarding professional perceptions of Digital Engineering that can inform future research and practice in information assurance and IT service delivery. The systems engineering approach to research design ensures traceability between research questions, survey instruments, and analytical approaches—demonstrating that the same disciplinary rigor that Digital Engineering brings to complex systems can be applied to academic research itself.

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

[14] 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

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

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

[17] 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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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.

[24] 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

[25] 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

[26] 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

[27] 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[77] S. Gil, 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. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.3305

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[117] 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.

[118] 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`

[119] 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`

[120] 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`

[121] 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`

[122] 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?

A.2 Survey Structure Aligned to Core Dimensions

Table A.2: Survey Section Structure

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

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

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

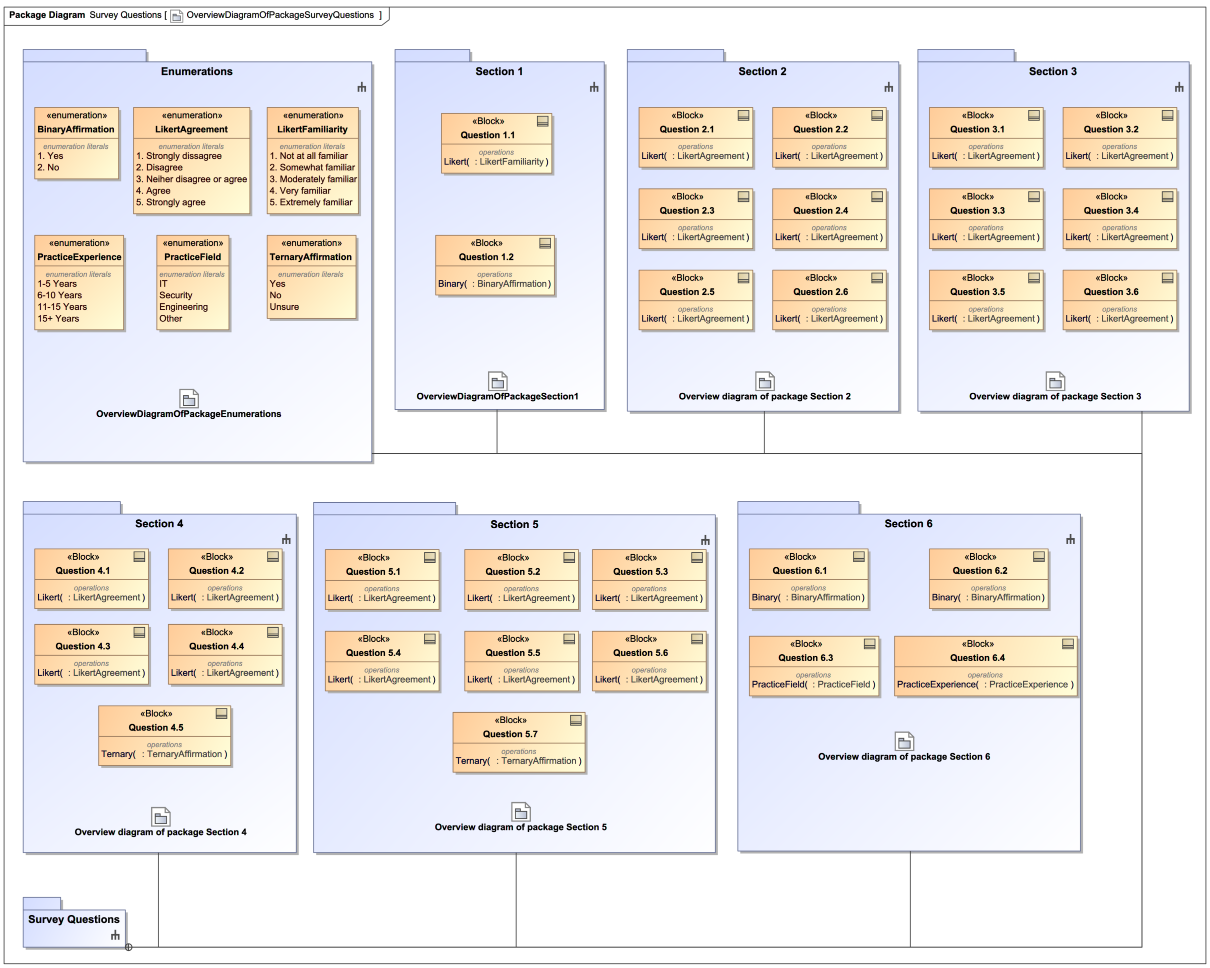


Figure A.1: Taxonomy of Survey Questions

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.