Research Report

RYAN CONSAUL, SARAH ZABEL, VANYA BARRER, CHRISTIAN KIM, ADRIAN SALAS, JOSHUA SIMULCIK, DRAKE WARREN

Independent Assessment of the Defense Business Enterprise Architecture

For more information on this publication, visit **www.rand.org/t/RRA3535-1**.

About RAND

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. To learn more about RAND, visit www.rand.org.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif.

Library of Congress Cataloging-in-Publication Data is available for this publication.

ISBN: 978-1-9774-1562-2

Limited Print and Electronic Distribution Rights

RR-A3535-1

About This Report

In Section 922 of the fiscal year 2024 National Defense Authorization Act, Congress directed the Secretary of Defense to commission an independent assessment of the effectiveness of the defense business enterprise architecture (DBEA) as a framework for planning, managing, and integrating defense business systems and its adequacy in informing business process reengineering. Congress also directed a comparison of the DBEA with similar models from other U.S. government agencies, foreign governments, and major commercial entities to identify lessons that could be applied to the DBEA. The U.S. Department of Defense (DoD) Office of the Chief Information Officer (CIO) contracted with the RAND National Defense Research Institute (NDRI) to conduct that assessment.[1] The results of the assessment are provided in this report.

The research reported here was completed in June 2025 and underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

National Security Research Division

This research was sponsored by DoD CIO and conducted within the Acquisition and Technology Policy Program of the RAND National Security Research Division (NSRD), which operates NDRI, a federally funded research and development center sponsored by the Office of the Secretary of Defense, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND Acquisition and Technology Policy Program, see www.rand.org/nsrd/atp or contact the director (contact information is provided on the webpage).

Acknowledgments

We are grateful to the numerous individuals in the office of DoD CIO, the Office of the Secretary of Defense, the services, and external organizations who contributed to the development of this report, responding to interview requests and providing documentation to us. We also thank our RAND colleagues who provided an "in-stride" review of our research and gave us a critical sounding board as we developed our approach, analysis, and conclusions. As always, we retain full responsibility for the quality of our research.

[1] On September 5, 2025, the President signed Executive Order 14347 to authorize the use of the name Department of War as a secondary title for the Department of Defense. This report was written before that order was released and thus refers to the secretary and department by their current statutory names.

Summary

Issue

In October 2004, under Title 10, Section 2222(e) of the U.S. Code,[2] Congress required the U.S. Department of Defense (DoD) to implement a defense business enterprise architecture (DBEA) to support the management of the department's business processes and systems.[3] Over the years, the DBEA has undergone numerous changes, including new versions, approaches, and transitions in leadership, which together have impacted its currency and utility. Concerns regarding the effectiveness of the DBEA in achieving its intended outcomes are evidenced by the U.S. Government Accountability Office's (GAO's) inclusion of the DBEA in its High Risk List area for DoD business systems modernization since 2011. Because of these continued concerns, Congress directed the Secretary of Defense to commission an independent assessment of the effectiveness of the DBEA as a framework for planning, managing, and integrating DoD business systems and its adequacy in informing business process reengineering. The fiscal year (FY) 2024 National Defense Authorization Act (NDAA) also directed a comparison of the DBEA with similar models in use by other government agencies in the United States, foreign governments, and major commercial entities to identify lessons that could be applied to the DBEA. This report provides results of this analysis to the Office of the DoD Chief Information Officer (CIO).

Approach

The following research questions guided our efforts to examine the effectiveness of the DBEA in its current form:

1. What does Title 10, Section 2222(e), direct DoD to do?
2. Does the current DBEA meet those requirements?
3. Do those requirements and the current DBEA provide an adequate framework for planning, managing, integrating, modifying, and transforming the defense business enterprise?
4. What needs to change?

The study team reviewed available documentation and open literature and interviewed key stakeholders. Specifically related to our assessment of the effectiveness of the DBEA, we reviewed the

[2] U.S. Code, Title 10, Armed Forces; Subtitle A, General Military Law; Part IV, Service, Supply, and Property; Chapter 131, Planning and Coordination; Section 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; Subsection (e), Defense Business Enterprise Architecture.

[3] On September 5, 2025, the President signed Executive Order 14347 to authorize the use of the name Department of War as a secondary title for the Department of Defense. This report was written before that order was released and thus refers to the secretary and department by their current statutory names.

statutory requirements in Title 10, Section 2222(e),[4] and DoD and service implementation guidance. We reviewed a variety of documentation on the DBEA from the sponsor, including historical documents, guidebooks, and other information. We examined relevant GAO reports, including past *High-Risk Series* on the DBEA. We interviewed stakeholders and conducted coding analysis of the interviews to identify key issues.

Two research questions guided our analysis of alternative approaches in the public sector:

1. Is there a different approach that would provide a better framework for planning, managing, integrating, modifying, and transforming the defense business enterprise?
2. How would DoD get there?

We identified the enterprise architectures and logic frameworks most relevant to the DBEA from international partners and allies. Our private sector analysis focused on identifying industry enterprise architectures and frameworks most relevant to the DBEA's mission for a baseline understanding of their components and lessons learned that could be applicable to DoD.

Key Findings and Recommendations

In January 2024, DoD CIO announced a new approach to modernizing the DBEA into a federated architecture framework.[5] This new framework uses the previous version of the DBEA (version 11.2) developed under the department's Chief Management Officer as a starting point but is designed with the intent to better empower defense business function leaders to manage their portfolios. Our study considered the DBEA as implemented by the end of 2023 and its progress during the period of the study.[6]

Our analysis led to the following key findings:

- DoD CIO's new federated architecture framework is a promising approach, but institutional inertia and a lack of compelling use cases have the potential to stall its momentum.
- The DBEA requires greater flexibility and stakeholder engagement to fulfill its purposes with respect to defense business systems and business process reengineering.
- Some of the legal specifications for the DBEA are overbroad and unhelpful.
- The new DBEA needs to mature through practical application before it will provide an adequate and useful framework for planning, managing, and integrating business systems of the department.

[4] Although the goals of U.S. Code, Title 10, Section 2222(e), relate to the broader goals of enterprise portfolio management embodied in Title 40 of the U.S. Code (also known as the Clinger Cohen Act), we framed our analysis around the goals specified in U.S. Code, Title 10, Section 2222.

[5] DoD, *Federated DoD Business Enterprise Architecture (BEA) Framework—Modernization of the DoD BEA*, January 2024a.

[6] Section 922 of the FY 2024 NDAA directs assessment of the DBEA "as of the date of the enactment of this Act," which was December 22, 2023. At that point in time, development and maintenance of the DBEA were in mid-transfer to a new system environment. Because of a lapse in system licenses, DoD CIO staff were unable to complete the transfer until several months later. Through the end of 2023 and into 2024, the governance bodies that use and support the DBEA were reconstituted, and a new approach to the DBEA was announced. Because the DBEA and the environment within which it exists were in a nonrepresentative state on December 22, 2023, this study includes progress made during 2024.

- The DBEA is not realizing its potential to inform business process reengineering, primarily because of an incentive structure focused on funding for information systems.

To address these findings, we recommend the following:

- The new DBEA needs relevant use cases to prove its value and inform its continued development. The approaching deadline for financial statement audit—and the wealth of business process and business system related challenges to success—make auditability an opportunity-rich area within which to pursue bounded use cases for the DBEA. **The Defense Business Council (DBC) should define initial use cases to address bounded problems necessary to prepare for financial statement audit.**
- The DBEA lacks analytic, visualization, and other tools necessary to inform decisionmaking. **DoD CIO should form a partnership with the Chief Digital and Artificial Intelligence Office to better enlist the Advana enterprise data and analytics environment in realizing the DBEA's full potential.**
- Stakeholders with operational needs that do not align well with current constructs need a nondisruptive way to interact with the DBEA. **DoD CIO should provide an experimentation space—a "sandbox"—to support flexibility for functional and mission alignment.**
- An experimentation space would also support testing new constructs from allied nations and industry. **DoD CIO should use the experimentation space to explore potential contributions from alternative models and frameworks.**
- The DBEA needs to adapt to emerging technologies. **DoD CIO should partner with DoD organizations, including the Defense Digital Service and Defense Innovation Unit, for active outreach to industry.**
- Interviewees and other sources report that the certification process is ineffective. **The DBC should redesign the annual certification process to be meaningful and publish clear guidance for its execution.**
- In its current form, the DBEA is not effective for planning, managing, and integrating business systems of the department. **DoD CIO should improve outreach, automation, and modernization of the DBEA.**
- In its current form, the DBEA is not adequate in informing business process reengineering for the department. **DoD CIO and the services should strengthen the ability of the DBEA to support business process reengineering efforts.** Detailed recommendations are provided in Chapter 5.

Enterprise architecture is a proven methodology for achieving the business process and system modernization goals specified in law. As the Army has shown, if managed effectively with appropriate governance, resources, and results-oriented focus, a business enterprise architecture can achieve the goals intended by Title 10, Section 2222.

Contents

Figures and Tables

Figures

Tables

Chapter 1

Introduction

The defense business enterprise architecture (DBEA) originated from the intent by Congress and U.S. Department of Defense (DoD) leadership to improve management of the department's financial and nonfinancial systems and business processes, thus improving stewardship of DoD's budget.[7] In 2004, Congress mandated a DBEA in a new Section 2222 of Title 10 of the U.S. Code, entitled "Defense business systems: architecture, accountability, and modernization."[8] The U.S. Government Accountability Office (GAO) has raised issues regarding the implementation of the DBEA, however, and has included DoD business systems modernization on its High Risk List since 1995, specifying the DBEA as a high-risk subarea since 2011. Given these concerns, Congress directed the Secretary of Defense to commission an independent assessment of the effectiveness of the DBEA and to identify lessons from similar models that could be applied to the DBEA. This report presents results of that assessment. The study was sponsored by the office of the DoD Chief Information Officer (CIO) in accordance with direction in Section 922 of the fiscal year (FY) 2024 National Defense Authorization Act (NDAA).[9]

Section 922 of the FY 2024 NDAA directed that a federally funded research and development center or a university affiliated research center conduct the independent assessment and required (1) an assessment of the DBEA's effectiveness in providing "an adequate and useful framework for planning, managing and integrating" DoD's business systems; (2) a comparison to and applicable lessons from similar models in use in other government agencies, foreign governments, and major commercial entities; (3) an assessment of the adequacy of the DBEA in "informing business process reengineering and being sufficiently responsive to changes in business processes over time;" (4) shortfalls or challenges of the DBEA; and (5) recommendations for the replacement or modification of the DBEA to better align with DoD's needs. The full text of Section 922 is included in Appendix A.

[7] On September 5, 2025, the President signed Executive Order 14347 to authorize the use of the name Department of War as a secondary title for the Department of Defense. This report was written before that order was released and thus refers to the secretary and department by their current statutory names.

[8] U.S. Code, Title 10, Armed Forces; Subtitle A, General Military Law; Part IV, Service, Supply, and Property; Chapter 131, Planning and Coordination; Section 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management; and Public Law 108-375, Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, October 29, 2004.

[9] Public Law 118-31, National Defense Authorization Act for Fiscal Year 2024; Section 922, Independent Assessment of the Defense Business Enterprise Architecture, December 22, 2023.

Research Questions and Approach

To address the NDAA language discussed above, we organized the study into two research tasks. The first task sought to characterize the current implementation of the DBEA against its statutory requirements. We used the following research questions to guide our efforts:

1. What does Title 10, Section 2222(e), direct DoD to do?
2. Does the current DBEA meet those requirements?
3. Do those requirements and the current DBEA provide an adequate framework for planning, managing, integrating, modifying, and transforming the defense business enterprise?
4. What needs to change?

To conduct our research for task 1, we reviewed the statutory requirements in Title 10, Section 2222(e), and DoD and service-level implementation guidance. We obtained and reviewed a variety of documentation on the DBEA from the sponsor, such as guidebooks, information describing DBEA end-to-end (E2E) processes, DBEA working group (WG) presentations, and recent guidance describing the new federated approach to the DBEA. We also reviewed historical information on prior versions of the DBEA. We examined relevant GAO reports, including past *High-Risk Series* on the DBEA, and analyzed guidance and other documents related to DoD's financial statement audit for past linkages to the DBEA. We interviewed key stakeholders and conducted coding analysis of the interviews to identify issues, as shown in Appendix B. We were also briefed on service approaches to business enterprise architecture (BEA).

The second task was to research alternative models to identify other information modeling approaches that might better serve the compliance, management, and transformation needs of DoD. For this task, two research questions guided our work:

1. Is there a different approach that would provide a better framework for planning, managing, integrating, modifying, and transforming the defense business enterprise?[10]
2. How would DoD get there?

To conduct our research for task 2, we bifurcated our search for analogous models and practices, looking at both the public sector (government-developed frameworks and architectures) and the private sector (industry led frameworks and architectures). Our public sector analysis involved identifying the most relevant enterprise architectures and logic frameworks to the DBEA from international partners and allies, focusing our efforts on the Five Eyes (FVEY) sharing consortium.[11] Our private sector analysis focused on identifying enterprise architectures and frameworks that are directly relevant to the DBEA's mission. We reviewed open source literature on these related frameworks for a baseline understanding of their components and lessons learned that could be applicable to DoD.

[10] Although we began task 2 with an open mind to approaches other than some form of enterprise architecture, because of time constraints and legal requirements specified in U.S. Code, Title 10, Section 2222, we chose to limit our assessment to alternative models that continue to adhere to enterprise architecture principles.

[11] In addition to the United States, the FVEY sharing consortium includes the United Kingdom (UK), Canada, Australia, and New Zealand.

Limitations of Our Approach

The study mandate asked us to conduct our assessment of the DBEA "as of the date of the enactment of this Act." Although we obtained information on the prior versions of the DBEA, our focus was on the current version. This scope posed challenges because the DBEA had not been fully utilized since its transition from the DoD Chief Management Officer (CMO) to DoD CIO, who in January 2024 called for a new federated approach to DBEA implementation. This new approach, changes in systems supporting access to the DBEA, and a gap in system licenses required to maintain the DBEA during the transition necessitated a substantial update to the DBEA during the time of our review. The resulting period of uncertainty and change affected interviewee experiences and limited the ability of the DBEA to inform decisionmakers.

To provide timely input for potential congressional action, we addressed alternative models through a literature review instead of by conducting interviews, thus limiting our understanding of the context and details around these alternative approaches. Rather than conducting an exhaustive search for similar models in use in other U.S. government agencies, we discuss the Army business enterprise architecture (ABEA) as a pertinent model applicable to DoD. To the extent feasible, the study team engaged with colleagues in RAND Europe and RAND Australia to obtain information about allied nation approaches.

Organization of This Report

Chapter 2 discusses the DBEA's statutory requirements and implementation guidance. Chapter 3 provides an overview of how the DBEA has been implemented in DoD in the areas of interoperable defense business system (DBS) solutions, business process reengineering efforts, and compliance. Chapter 4 describes applicable lessons from our literature review of partner nations and industry approaches to enterprise architecture. Chapter 5 presents our findings and recommendations.

Appendix A includes the statutory language directing our study. Appendix B provides an overview of our interview coding analysis and approach. Appendix C describes the governance of the DBEA. Appendix D describes the ABEA. Appendix E provides background information on DoD's financial statement audit. Finally, Appendix F discusses industry enterprise architecture approaches reviewed.

Chapter 2

The Evolution of the DBEA to the Present

Definitions and Attributes of a BEA

During this analysis, we sought to understand the basic foundations of an architecture for an enterprise, the reasons for having an architecture, and the implications of creating and maintaining one. However, we learned very quickly that *architecture* is not a one-size-fits-all solution but rather a construct that must be tailored to the organization's capabilities, needs, and goals. In short, an architecture is an abstraction of the real world. Architects model salient characteristics of that world and can then project alternatives and estimate impacts to operational effectiveness, efficiency, and other factors.

There are various terminologies to describe an organization's architecture, with *enterprise architecture* (EA) and *business architecture* (BA) being primary. To account for the different definitions, interpretations, and attributes that describe BA and EA, we provide select examples from academia and industry in Table 2.1.[12] Additionally, *enterprise business architecture* focuses on nontechnical components and processes of an organization that relate to business strategy, such as policies, human resources, and modeling, and helps inform the technological necessities.[13] *Business enterprise architecture* aligns processes, systems, and overall business strategies.[14] Despite these differences, we can posit key attributes that all architectures must have:

- An architecture is a blueprint of a set of activities and components (e.g., systems, standards, personnel) created based on the needs of the organization.
- An architecture must be developed and maintained such that there is a clear inventory of components and capabilities, so that changes or improvements can be made as needed.

Architecture is not a one-size-fits-all approach. Every organization, whether commercial, governmental, or nonprofit, stems from different industries, comprises different activities and components, and pursues distinct goals. Ramifications of these varying definitions, interpretations, and attributes of architectures on the DBEA imply that because of the size, scale, and mission needs of DoD, it cannot simply look to other organizations in industry or other federal government agencies

[12] Note that organizations can have different definitions, interpretations, and descriptions of attributes while using the same terminology. Definitions can be similar for different terminologies and differ for the same terminologies.

[13] Tiko Iyamu and Irja Shaanika, "The Factors of Enterprise Business Architecture Readiness in Organisations," *Enterprise Information Systems*, 2022.

[14] Dongwoo Kang, Jeongsoo Lee, and Kwangsoo Kim, "Alignment of Business Enterprise Architecture Using Fact-Based Ontologies," *Expert Systems with Applications*, Vol. 37, No. 4, April 2010.

for applicable examples to develop and maintain a suitable architecture. The resources and strategic priorities of DoD will be different from organizations in private industry, such as Amazon and Walmart.

Table 2.1. Variances in Describing Architecture

Source	Term	Key Features
"Actionable Business Architecture"[a]	BA	• This source defines BA as a framework representing the relationship between the strategy, operations, and information technology (IT) aspects of an organization. • The strategy side focuses on ensuring that the organization can meet its goals, maintain its competitive posture, and transform its operations and goals as needed. • The operations side deals with business process management and the execution of everyday functionalities. • The IT side focuses on the technological infrastructure and operations in terms of its ability to produce technical services across the organization.
"The Use of Artificial Intelligence Technologies in Building Business Architectures Within Framework of the 'Green Economy'"[b]	BA	• The primary focus of this source is using artificial intelligence (AI) technologies in studying business architectures to optimize management processes. • This source defines BA as a broad component of an organization's EA to organize and represent an organization's processes and elements. • The BA model primarily comprises the business unit architecture, information architecture, information system architecture, data architecture, and delivery system architecture, with each component playing a specific relational role with one another.
"Defining Enterprise Architecture: A Systematic Literature Review"[c]	EA	• This source focuses on the ways in which EA is defined and discussed, especially given that the source acknowledges that there is no common baseline of a definition. • One example shows that EA can be defined as it relates to its components, specifically that it is an infrastructure that consists of an organization's critical components, their relationships to one another, and the ways in which they interact in internal and external environments. • Another example shows that EA can be defined in terms of its role as a tool, specifically that it consists of models, methods, and policies that represent the organization's structure and processes.
Building Value Through Enterprise Architecture: A Global Study[d]	EA	• This source defines EA as a framework that aligns an organization's goals and priorities with their everyday operations and technological capabilities. • Critical attributes include clearly outlining the organizational structure in business and IT roles, ensuring interoperability and standardization of information, and ensuring that all integrated infrastructure and efforts support business operations and goals. • EA can help the organization both in the short term (e.g., budgeting, managing business portfolio and assets, developing relationships with internal and external personnel) and long term (e.g., interoperability across the organization, maintaining a high degree of agility to changing conditions, maintaining efficient operations).

[a] Ray Harishankar and S. Kevin Daley, "Actionable Business Architecture," paper presented at 2011 IEEE Conference on Commerce and Enterprise Computing, 2011.

Source	Term	Key Features

[b] Elena V. Lukashina, Alexandr V. Lukashin, and Valery I. Bezrukov, "The Use of Artificial Intelligence Technologies in Building Business Architectures Within the Framework of the 'Green Economy,'" *International Scientific Conference Energy Management of Municipal Facilities and Environmental Technologies*, Vol. 458, 2023.
[c] Patrick Saint-Louis, Marcklyvens C. Morency, and James Lapalme, "Defining Enterprise Architecture: A Systematic Literature Review," paper presented at 2017 IEEE 21st International Enterprise Distributed Object Computing Conference Workshop, 2017.
[d] Peter Burns, Michael Neutens, Daniel Newman, and Tim Power, *Building Value Through Enterprise Architecture: A Global Study*, Booz & Company, 2009.

Therefore, although these definitions provide a glimpse of the differing interpretations to describe the components and processes of an architecture, DoD cannot rely on them for guidance on how to best develop and maintain an architecture to meet its needs.

Origins of the Defense BEA

DoD's responsibility to develop and maintain an IT architecture was initiated with the Clinger Cohen Act (CCA) of 1996. This act established CIO positions for DoD and other federal agencies, with responsibilities that included "developing, maintaining, and facilitating the implementation of a sound, secure, and integrated information technology architecture for the executive agency" that they served.[15] Incorporated now in Title 40 of the U.S. Code, the law defines an IT architecture as "an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals."[16] The overall purpose of the CCA is to lower costs and improve efficiency throughout the federal government. The act does not call out business systems in particular but applies to all the department's IT investments.

The FY 1998 NDAA added a Section 2222 to Title 10 of the U.S. Code to mandate a "biennial financial management improvement plan" from the department.[17] The focus of Section 2222 at that time was to bring order to the Pentagon's finances, and although Section 2222 addressed "all aspects of financial management within the Department of Defense including the finance systems, accounting systems, and data feeder systems," it did not explicitly direct the development of an architecture. The FY 2002 NDAA revised the biennial plan to an annual plan and directed the "establishment and maintenance of a complete inventory of all budgetary, accounting, finance, and data feeder systems," as well as "a phased process for improving systems that includes mapping financial data flow."[18]

[15] Public Law 104-106, National Defense Authorization Act for Fiscal Year 1996; Division E, Information Technology Management Reform, February 10, 1996.

[16] U.S. Code, Title 40, Public Buildings, Property, and Works; Subtitle III, Information Technology Management; Chapter 113, Responsibility for Acquisitions of Information Technology; Subchapter II, Executive Agencies; Section 11315, Agency Chief Information Officer; Subsection B; Paragraph 2.

[17] Public Law 105-85, National Defense Authorization Act for Fiscal Year 1998, Division A, Department of Defense Authorizations; Title X, General Provisions; Section 1008, Biennial Financial Management Improvement Plan; Subsection a, Paragraph 1, November 18, 1997.

[18] Public Law 107-107, National Defense Authorization Act for Fiscal Year 2002, Division A, Department of Defense Authorizations; Title X, General Provisions; Subtitle A, Financial Matters; Section 1009, Financial Management Modernization Executive Committee and Financial Feeder Systems Compliance Process; Subsection c, Paragraphs 1 and 2, December 28, 2001.

According to Peter Levine in his book *Defense Management Reform: How to Make the Pentagon Work Better and Cost Less*, these NDAA requirements reflected a long standing frustration in Congress of perceived out-of-control spending by the Pentagon. In particular, the Chief Financial Officer Act of 1990 required that DoD be subject to a financial statement audit, and the Government Management Reform Act of 1994 made the financial statement audit an annual requirement. Pressed by GAO in 2000 and 2001 and faced with the repeated failure of the department to achieve an unmodified opinion on its financial statements, Secretary of Defense Donald Rumsfeld directed the department to develop "a DoD-wide blueprint—an enterprise architecture . . . —that prescribes how the Department's financial and nonfinancial feeder systems and business processes will interact."[19] Title 10, Section 2222, was repealed in 2002, and a new Section 2222, entitled "Defense business systems: architecture, accountability, and modernization," was added two years later.[20]

Over the years, the text of Title 10, Section 2222, has changed considerably, establishing and changing processes for business management and reform, implementing initiatives, and revising responsibilities among the organizations involved. Business systems covered by the law expanded to include "financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure, used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management."[21] Throughout the years since its reestablishment, though, each version has maintained a consistent set of requirements for a DBEA, shown in Table 2.2.

Table 2.2. Statutory Requirements for Defense Business Enterprise Architecture

U.S. Code	Relevant Legal Specifications
Title 10, Section 2222	**Defense business systems: business process reengineering; enterprise architecture; management** (e) Defense Business Enterprise Architecture. (1) Blueprint. The Secretary, working through the Chief Information Officer of the Department of Defense, shall develop and maintain a blueprint to guide the development of integrated business processes within the Department of Defense. Such blueprint shall be known as the "defense business enterprise architecture". (2) Purpose. The defense business enterprise architecture shall be sufficiently defined to effectively guide implementation of interoperable defense business system solutions and shall be consistent with the policies and procedures established by the Director of the Office of Management and Budget. (3) Elements. The defense business enterprise architecture shall- (A) include policies, procedures, business data standards, business performance measures, and business information requirements that apply uniformly throughout the Department of Defense; and (B) enable the Department of Defense to

[19] Peter Levine, *Defense Management Reform: How to Make the Pentagon Work Better and Cost Less*, Stanford University Press, 2020, p. 187.

[20] Public Law 107-314, Bob Stump National Defense Authorization Act for Fiscal Year 2003, December 2, 2022; Public Law 108-375, 2004.

[21] Public Law 108-375, 2004.

U.S. Code	Relevant Legal Specifications
	(i) comply with all applicable law, including Federal accounting, financial management, and reporting requirements; (ii) routinely produce verifiable, timely, accurate, and reliable business and financial information for management purposes; (iii) integrate budget, accounting, and program information and systems; and (iv) identify whether each existing business system is a part of the business systems environment outlined by the defense business enterprise architecture, will become a part of that environment with appropriate modifications, or is not a part of that environment. (4) Integration into information technology architecture. (A) The defense business enterprise architecture shall be integrated into the information technology enterprise architecture required under subparagraph (B). (B) The Chief Information Officer of the Department of Defense shall develop an information technology enterprise architecture. The architecture shall describe a plan for improving the information technology and computing infrastructure of the Department of Defense, including for each of the major business processes conducted by the Department of Defense. (5) Common enterprise data. The defense business enterprise shall include enterprise data that may be automatically extracted from the relevant systems to facilitate Department of Defense-wide analysis and management of its business operations.
Title 10, Section 2222	(i) Definitions. In this section: (1)(A) Defense business system. The term "defense business system" means an information system that is operated by, for, or on behalf of the Department of Defense, including any of the following: (i) A financial system. (ii) A financial data feeder system. (iii) A contracting system. (iv) A logistics system. (v) A planning and budgeting system. (vi) An installations management system. (vii) A human resources management system. (viii) A training and readiness system. (B) The term does not include- (i) a national security system; or (ii) an information system used exclusively by and within the defense commissary system or the exchange system or other instrumentality of the Department of Defense conducted for the morale, welfare, and recreation of members of the armed forces using nonappropriated funds.
Title 44, Section 3601	**Definitions** In this chapter, the definitions under section 3502 shall apply, and the term (4) "enterprise architecture" (B) includes (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan

SOURCES: U.S. Code, Title 10, Section 2222; U.S. Code, Title 44, Public Printing and Documents; Chapter 36, Management and Promotion of Electronic Government Services; Section 3601, Definitions.

The specification of the DBEA today reflects its dual heritage. Though it integrates with—but does not replace—the IT enterprise architecture still required in Title 40, it maintains the CCA drive to guide modernization of DoD's business processes and systems. At the same time, its emphasis on compliance with law and regulation and production of financial and business data reflect its origins in the efforts to make DoD auditable. Those goals are not necessarily compatible. Business system and process modernization is forward-looking to a new end state, inviting conjecture and experimentation, while goals for financial statement audit and compliance imply deep visibility and rigid control of the current state. In his treatment of the history of attempts to audit the Pentagon, Levine paints the architectural approach as a failed "grand design," commenting that "The BEA . . . suffered from the overambitious objective of trying to comprehend all the details and all the defects of the department's business systems before trying to address any of them."[22]

The form of the defense BEA and responsibility for its development also went through changes over the years. The earliest predecessor of the DBEA was the Financial Management Enterprise Architecture, sponsored by the Under Secretary of Defense (Comptroller) within the Financial Management Modernization Program (FMMP).[23] In 2003, the FMMP was renamed to the Business Management Modernization Program and its architecture to the Business Enterprise Architecture (BEA) to avoid the appearance of sole focus on financial processes and systems.[24] In 2005, the BEA was placed under the control of the Business Transformation Agency (BTA), which operated under the authority and direction of the DBS Management Committee, chaired by the Deputy Secretary of Defense.[25]

Under BTA management, the BEA was expanded to map to the laws, regulations, and policies (LRPs) impacting DoD business operations and linked to an enterprise transition plan. The purpose of the BEA at that point was to define standards to drive transformation across the department and to support portfolio management and acquisition decisions regarding DBSs. E2E process descriptions were added to contextualize architectural content adhering to reference models within the Department of Defense Architecture Framework (DODAF).[26]

Organizational responsibility for development of the DBEA changed hands several more times in the years that followed. In 2012, the BTA was dissolved and responsibility for the defense BEA transferred to a new Deputy Chief Management Officer (DCMO) of DoD.[27] The office of the DCMO was dissolved in 2018 and responsibility transferred to a new CMO, and that office was dissolved in 2021.[28] At that time, responsibility for the DBEA was transferred to DoD CIO, where it remains at the time of this study.[29]

---

[22] Levine, 2020, p. 194.

[23] Donald Rumsfeld, "Financial Management Information Within the Department of Defense," memorandum, U.S. Department of Defense, July 19, 2001.

[24] Christopher Hanks, "A Critical Examination of the DoD's Business Management Modernization Program," *Proceedings of the Second Annual Acquisition Research Symposium*, Naval Postgraduate School, May 1, 2005.

[25] Public Law 108-375, 2004.

[26] Amr Sabet, "BEA History," briefing slides, Infinit-EA, undated.

[27] Sabet, undated.

[28] Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, August 13, 2018.

[29] Public Law 117-263, James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, December 23, 2022.

Through its later years, the DBEA was hosted on a publicly available website. According to interviewees, system licenses for its maintenance were not renewed, and the public website was discontinued because of security concerns. BEA version 11.2, released in 2020, was ported to an internal DoD website, where it exists now. Parts of the architecture have been re-created on an Army-owned instance of ARIS,[30] and, at the time of this study, DoD components still align to BEA 11.2 through the DITPR for the annual certification process.

Reconceptualization of the DBEA Under DoD CIO and Recent Developments

In January 2024, the Deputy CIO for Information Enterprise issued a new federated approach to the DBEA,[31] recognizing that the BEA had helped drive the integration of business operations through data and process standards but "has not been used for its intended purpose" in other areas.[32] The approach sought to modernize the DBEA and utilize a segmented architecture methodology to focus on DBS optimization and rationalization opportunities and allow flexibility for DoD components to continue portfolio management efforts. The new federated DBEA leverages the most recent version of the DBEA (version 11.2) as a starting point but transitions to "an agile, questions-based approach focused on defined requirements and specific data needs of DBEA stakeholders."[33] It is designed to enable decisionmakers to visualize DBS rationalization opportunities, address compliance, and depict process inefficiencies.[34]

According to the January 2024 document, the new federated DBEA is composed of three categories of segment architectures: an enterprise segment, a component segment, and an initiative segment. Although the segments are distinct, together they allow for a holistic view of DBSs across the department. Seventeen E2E major business processes form the foundation of the architecture.[35] These

[30] ARIS is a software platform within the Army's Enterprise Knowledge Repository that maintains the BEA and is accessible to DoD components for their component and initiative segments. The Defense Information Technology Portfolio Repository (DITPR) includes DBS alignment to some aspects of the BEA. See DoD, *Department of Defense Business Enterprise Architecture Guidebook*, 2024b.

[31] According to GAO, the DBEA first adopted a federated model within which each DoD component would develop and maintain its own conforming enterprise architecture in September 2006. GAO described a federated architecture as "a family of coherent but distinct member architectures that conform to an overarching architectural view and rule set. . . . Under a federated approach, member architectures are substantially autonomous, although they also inherit certain rules, policies, procedures, and services from higher-level architectures. As such, a federated architecture enables component organization autonomy, while ensuring enterprise-wide linkages and alignment where appropriate" (GAO, *Business Systems Modernization: Strategy for Evolving DOD's Business Enterprise Architecture Offers a Conceptual Approach, but Execution Details Are Needed*, GAO-07-451, April 2007, p. 8). When we refer to the new federated architecture in this report, it is to deconflict with the previous released version commonly known as BEA 11.2.

[32] DoD, *Federated DoD Business Enterprise Architecture (BEA) Framework—Modernization of the DoD BEA*, January 2024a, p. 3.

[33] DoD, 2024a, p. 4.

[34] DoD, 2024a, pp. 4–5.

[35] The E2E processes documented in the federated BEA approach document are Acquire-to-Retire—Equipment; Acquire-to-Retire—Real Property; Budget-to-Report; Concept-to-Product; Cost Management; Deployment-to-Redeployment Retrograde; Environmental Liabilities; Excess-to-Disposal; Hire-to-Retire; Market-to-Prospect; Order-to-Cash; Plan-to-Stock; Procure-to-Pay; Proposal-to-Reward; Request-to-Delivery; Service Request-to-Resolution; and Service-to-Satisfaction. During the course

E2E processes, delineated at the first level as process steps, relate to operational activities (OAs) that "describe the individual activities, tasks, and business functions performed within each E2E"[36] and are decomposed to deeper levels. Component segments map functional business areas and conform to the enterprise segment's E2E processes and OAs. Initiative segments can be created "to address particular business questions or portfolio management priorities."[37] This structure supports consistency across architecture segments, traceability with LRPs, and portfolio management. DoD CIO has drafted a guidebook with information on several important topics, including roles and responsibilities, governance, tools (including Enterprise Knowledge Repository, DITPR, and Advana[38]), procedures for intake and change management, and use cases. At the beginning of this study, 17 E2Es had been identified, building on the 15 E2Es in version 11.2. Process champions established a catalog of OAs and LRPs, such that all OAs map to at least one E2E process step.

Within the federated architecture, the maturity of individual component BEAs varies greatly. The ABEA, described in Appendix D, is the most mature and actively used in managing its business system portfolio. The Navy actively uses its BEA for a business system rationalization effort, called Cattle Drive. We spoke with several Office of the Secretary of Defense (OSD) staff elements that were in early stages of working across services and defense agencies to bring together a cohesive picture of their functional area in a segment BEA, but we did not find any other segments of the DBEA in active use to support decisionmakers. Most interviewees conveyed to us that they interacted with the DBEA only to comply with Title 10, Section 2222.

The DBS Cross Functional Board (CFB) was created under the oversight of the Defense Business Council (DBC) to oversee the implementation of the federated DBEA approach and act as the DBEA's configuration control board, and an action officer level BEA WG was established to facilitate the modernization of the DBEA. (Additional information on governance bodies overseeing the DBEA can be found in Appendix C.)

The DBEA WG established aggressive time frames to define E2Es, identify and define OAs and relevant LRPs, map those constructs to one another, and operationalize the DBEA.[39] These activities were delayed because of competing priorities and varied progress across the functional areas in populating the DBEA with necessary data and information, as well as internal disagreements regarding the modernization approach. As of the release of this report, the DBEA had yet to realize the vision for the new federated approach.

---

of our study, DoD officials discussed adding one E2E process, for a total of 18. However, a final decision had not been made as of this report's release (September 2025).

[36] DoD, 2024a, p. 6.

[37] DoD, 2024a, p. 7.

[38] The Advancing Analytics (Advana) platform is operated by the DoD Chief Digital and Artificial Intelligence Office (CDAO). It is DoD's enterprise data and analytics environment and provides DoD users with data from more than 400 DoD business systems, along with tools, services, and analytics to enable data-based decisionmaking (CDAO, "Analytic Tools," webpage, undated). According to the draft guidebook, Advana will incorporate ARIS content with other information on DBSs for use as an enterprise data management and analytics platform. See DoD, 2024b. Enterprise Knowledge Repository is a digital repository of tools and data used by members of the Army's acquisition community to enhance their ability to make data-supported decisions on programs and portfolios by creating reports, dashboards, and related schemes. DITPR is a database inventory of DoD's mission-critical and mission-essential IT systems and their interfaces to support Title 40/CCA requirements.

[39] Sarah Nather, "BEA Development and Implementation Way Forward," briefing slides, U.S. Department of Defense Chief Information Officer, March 2024.

The delay in fully modernizing the DBEA has created a void in which the DBC cannot use a completed DBEA to inform decisions. DoD officials we interviewed noted a lack of direction during the change of administrations, ending only after appointment of an acting DoD CIO. Without a demand signal from the DBC, the DBS CFB and BEA WG lacked the urgency needed to drive progress in modernizing the DBEA. Furthermore, the expansive scope of the E2Es, which span all DoD business functions, created significant complexities. DoD CIO, playing primarily a coordination role, was limited in its scope and instead relied on other key stakeholders, such as the E2E process champions, to drive progress. However, these stakeholders were not accountable to DoD CIO for the progress, or lack thereof, with the DBEA. This lack of accountability created challenges for this structure to govern the DBEA effectively and achieve modernization goals.

In February 2025, GAO released its latest High Risk List report, which identifies government programs and activities at greatest risk of fraud, waste, abuse, and mismanagement.[40] Its latest report continued to include DoD business systems modernization as a high risk area and, within it, a subarea for DoD's federated BEA. Since its 2023 update, GAO has improved ratings in three of five criteria used to measure progress across high risk areas: leadership commitment, action plan, and monitoring.

Despite recent progress, DoD business systems modernization has been on GAO's High Risk List since 1995, and the DBEA has been on the list since 2011. In its 2011 report, GAO noted that its "work has highlighted challenges that DOD still faces in aligning its corporate architecture and its component organization architectures, leveraging the federated architecture to avoid investments that provide similar but duplicative functionality in support of common DOD activities and institutionalizing the business systems investment process at all levels of the organization."[41] GAO has continued regular reporting on DoD's modernization efforts. In 2015, GAO also released a more detailed review of efforts associated with the DBEA and business process reengineering initiatives.[42] GAO also issued a report in 2023 on DoD's efforts to oversee and improve its business and financial systems to include efforts related to the DBEA.[43]

[40] GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743, February 2025.

[41] GAO, *High-Risk Series: An Update*, GAO-11-278, February 2011, p. 68.

[42] GAO, *DOD Business Systems Modernization: Additional Action Needed to Achieve Intended Outcomes*, GAO-15-627, July 2015.

[43] GAO, *Financial Management: DOD Needs to Improve System Oversight*, GAO-23-104539, March 2023a.

Chapter 3

The DBEA's Impact on Directed Outcomes

The totality of Title 10, Section 2222, in the U.S. Code emphasizes three overlapping areas of intended utility for the DBEA: modernizing DBSs, enabling business process reengineering, and supporting financial statement audit. That last intended use is derived from a combination of the origins of the DBEA and the enduring direction to enable compliance with all applicable laws; produce business and financial information; and integrate budget, accounting, and program information and systems. The observations presented below are based on a combination of interviews with current subject matter experts (SMEs) specializing in defense business architecture and a historical analysis of the DBEA effort. These insights reflect both contemporary experiences with the DBEA's implementation and broader lessons learned over time. By examining the perspectives of architecture SMEs alongside the historical trajectory of the DBEA, we can highlight successes, challenges, and opportunities in achieving each area of intended utility described in statute.

Modernization of DBS Solutions

The DBEA is intended to serve as a critical framework for guiding the development, modernization, and integration of DBSs by enhancing efficiency, interoperability, and compliance. By providing a structured approach, the DBEA aims to ensure that DBSs can interface effectively, integrate seamlessly into the broader defense ecosystem, and adhere to statutory and regulatory requirements. Additionally, the DBEA seeks to support strategic decisionmaking, improve cost efficiency, enhance data security, and enable life cycle management of systems. Past and current iterations of the DBEA have had mixed success in supporting the development and reengineering of integrated business processes. Early versions of the DBEA in the mid-2000s focused heavily on standardization, which helped establish a common language and framework across DoD components but often failed to account for the unique operational needs of individual services and functions. This rigidity has continued to hinder innovation and customization, limiting the ability of process owners to adapt the architecture to their specific requirements. Current iterations of the DBEA and its component BEAs have made strides in addressing these shortcomings by incorporating modular and scalable approaches, enabling greater flexibility in system design and integration. A recent and highly visible example of this increased flexibility is the January 2024 federated approach.[44] However, challenges remain, particularly in aligning service-specific architectures with enterprise-wide goals and ensuring that modernization efforts keep pace with emerging technologies. The complexity introduced

[44] DoD, 2024a.

by the large number of systems across both services and functions (1,337 as of December 2024) only exacerbates these challenges.[45] The DBEA continues to evolve under CIO's most recent pivot to using a federated approach across the department, but its ability to fully support integrated business systems depends on balancing technical and data standardization with adaptability and collaboration to account for business process differences and changes across stakeholders.

The observations presented in this section present challenges and opportunities with respect to interoperability, integration, compliance, cost efficiency, data security, strategic decisionmaking, modernization, life cycle management, and functional alignment of relevant DBSs.

Interoperability

The DBEA includes business data standards and information requirements for system development to ensure interoperability among DBSs. This is critical for reducing "collisions" that occur when systems fail to communicate effectively. Our interviewees emphasized the importance of avoiding isolated development efforts to prevent such collisions. As an enterprise-wide unified architecture, the DBEA has the ability to ensure that systems developed by different services can interface effectively through data models and common technical standards or protocols such as those promulgated by the DoD CIO Fulcrum strategy,[46] reducing duplication and enhancing operational efficiency. Incorporating legacy systems into modern architectures has allowed the business functions to continue using their established knowledge and procedures related to existing systems while modernizing their technology infrastructure, ensuring continuity of support. However, ensuring interoperability among legacy systems adds complexity and cost to programs, highlighting the need for better integration strategies and strategic decisions regarding modernization. In a constrained budget environment, some of that cost must be met by budget that could otherwise be used to accelerate modernization efforts and innovation.

System Integration

The DBEA's E2E processes and data standards aim to streamline the integration of new systems into the existing defense business ecosystem while allowing for flexibility by using segment architectures for detailed process steps.[47] Integration is viewed as essential for modernization efforts. Multiple interviewees familiar with DoD modernization efforts emphasized their desire for architected and trusted enterprise datasets that could better inform decisions. Despite the standardization provided by the DBEA, differences in lower level processes and service-specific variations can undermine the consistency required for true integration. In several of the interviews we conducted, we observed a cultural perception that military service processes continue to represent sufficiently unique requirements that full integration cannot be achieved without significant (and

[45] DoD IT Portfolio Repository, "Defense Business Systems Data Report," spreadsheet, December 2024.

[46] Fulcrum, the DOD CIO IT advancement strategy, is detailed in DoD, *Fulcrum: The Department of Defense Information Technology Advancement Strategy*, undated.

[47] DoD, 2024a.

perhaps unjustifiable) work. Although the DBEA has facilitated collaboration by providing a common system integration framework, a continuing shortfall in cross-service collaboration and department-wide reforms was also noted in GAO's 2023 *High-Risk Series* report.[48] Within the services, the documentation and compliance-checking associated with the integration framework has also been identified as introducing undesirable administrative overhead and slowing system deployment.

Compliance

The DBEA provides a structured compliance framework intended to ensure that DBSs meet federal laws, DoD policies, and standards. However, gaps exist between the DBEA's capabilities and the implementation guidance provided to system owners. Without clear guidance, several interviewees noted that compliance just becomes a box-checking exercise, indicating poor stakeholder engagement and insufficient education and awareness regarding the DBEA. Additionally, compliance processes introduce significant administrative overhead, adding to program costs. Centralizing data and improving transparency among DoD's business systems dataset will prepare the department for financial statement audit readiness, once the administrative burdens are reduced and stakeholders are engaged fully in a streamlined DBEA.

Cost Efficiency

Concerns were raised regarding the cost efficiency of maintaining outdated systems and the approach to commercial off-the-shelf (COTS) solutions. DoD's current approach to using COTS solutions is perceived as being primarily to consolidate current requirements that describe the as-is system rather than accounting for emerging or anticipated requirements that inform the to-be system. This highlights the need to reassess modernization strategies to enhance cost effectiveness. Although DBEA standardization has been credited for reducing duplicative spending by leveraging economies of scale and providing road maps for cost effective solutions, smaller programs can struggle to allocate sufficient resources to meet enterprise-wide requirements.

Data Security

The DBEA incorporates cybersecurity principles from broader architectures, such as the National Institute of Standards and Technology, to protect data and information. Interviewees expressed concerns about vulnerabilities arising from noncompliance with evolving security requirements and the challenges of adopting modern software development practices, such as agile methodologies. Legacy security practices may hinder iterative development, adding resource burdens to programs later in their life cycles. Delays in security updates introduce vulnerabilities to systems that fail to keep pace, also exposing military networks to greater risk.

[48] GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203, April 2023b.

Strategic Decisionmaking

In places, the DBEA provides consolidated access to defense business process and system data, serving as a decision support tool. However, this support is not yet realized across the defense business enterprise. Although it enables strategy-informed decisions, operational level metrics within the DBEA ecosystem are insufficient for measuring systems' impacts on more abstract strategic goals.[49] Interviewees did identify a current trend of increasing cross-functional collaboration in some of the defense business functions that should continue, supported by the DBEA's capability of enabling strategic alignment across functions. With greater awareness between services, functional leaders could make more strategic business decisions that could support intradepartmental convergence over time.

Modernization

The DBEA is intended to support modernization by identifying opportunities to integrate relevant aspects of legacy systems and processes into commercial best practices and solutions while supporting such cutting-edge technologies as cloud solutions, AI, and machine learning (ML). DBS modernization directs investment to support continuous value creation for the business functions and for leaders within DoD and the services. In addition to the systems, however, the framework itself must be updated to accommodate these and other emerging technologies. Interviewees highlighted challenges in modernizing legacy systems, highlighting resource constraints and technical difficulties. This observation and others underscore the need for continuous updates to software systems in the modern cyber context. Regardless of whether DoD is leveraging commercial software per the DBEA or developing its own through the Software Acquisition Pathway of the Adaptive Acquisition Framework, the need for active management and sustained investment has been well documented.[50] There remains a tension between traditional and modern approaches to software acquisition, and the DBEA has struggled to relieve that tension.

System Auditability

The auditability of business systems is supported by the DBEA's centralization of business process and system data, the alignment of its compliance frameworks to system audit requirements, and the timeliness of its near-real-time access to reports. Auditability is closely tied to compliance, because compliance with auditability requirements is one of the DBEA's primary purposes. However, while this centralized control of processes and data requirements helps ensure consistency and allow for comparison across the department, it can make it more difficult to adapt workflows or reports for specific types or scales of audits. For example, a logistics audit focused on inventory management and

[49] For instance, the *2022 National Defense Strategy* reads, in part, "we will better align requirements, resourcing, and acquisition" (DoD, *2022 National Defense Strategy of the United States of America*, 2022). An example metric that could be implemented in support of this strategic goal is a requirements adjustment rate to measure the frequency of post-validation changes that might signal system misalignment or a failure to integrate emerging technologies.

[50] Defense Acquisition University, "Adaptive Acquisition Framework Document Identification: Software Acquisition Pathway (SWP)," webpage, undated.

supply chain efficiency may need data reported in a different format or localized visualizations to more effectively identify risks and vulnerabilities. Although shared data can increase transparency and collaboration, the DBEA lacks the capacity to allow localized data manipulation to get after specific functional or other stakeholder emerging requirements without making modifications that have effects across the enterprise. When audits identify deficiencies or nonconformances in business systems' execution of documented business processes, the nature of centrally managed standardization like the DBEA drives a requirement for systematic review and remediation, which can slow the response time and can reduce the effectiveness of audits as a tool for continuous improvement.

Life Cycle Management

The DBEA supports life cycle management by aligning with the DoD systems engineering life cycle. Interviewees identified unnecessary redundancy in system capabilities as a challenge that has been aided by the DBEA and service-specific BEAs. However, the varying success between services in this area stems from differences in their implementation. Although the Army and Navy have reportedly succeeded in using their BEAs to sunset legacy systems, other components have had limited success retiring outdated systems. Changes in the systems engineering processes implemented over time create inconsistencies between management systems that are difficult to reflect in a centralized framework like the DBEA. Similarly, compliance requirements evolve over time and create their own inconsistencies and challenges. The DBEA lacks the ability to reflect the determined acceptability of each change within the broader context of the enterprise ecosystem, as well as what conditions would constitute a breach of that acceptability.

Functional and Mission Alignment

By mapping DBSs to functional needs and mission objectives, the DBEA seeks to ensure continual operational efficiency in support of warfighter readiness as far as DoD's strategic objectives can be reflected in actionable metrics. The framework struggles to address rapid shifts in priorities and inform necessary adjustments to business systems. However, aligning operational output with strategic objectives is critical. Previous versions of the DBEA documented this focus on outcomes through its Integrated Business Framework—Data Alignment Portal online tool, which housed functional strategies and organizational execution plans designed to support alignment with strategic objectives. The need for labor to manually organize large amounts of data into ingestible form, as well as the need to enter those same data into more than one system, was a finding in a 2012 GAO report.[51] We also heard similar issues to these in our interviews for this study, which lead to practical and cultural challenges in entering and maintaining the continuously updated data needed to make good mission-informed decisions.

[51] GAO, *DOD Business Systems Modernization: Governance Mechanisms for Implementing Management Controls Need to Be Improved*, GAO-12-685, June 2012.

Integrated Business Process Development and Reengineering

Under the direction of Title 10, Section 2222, defense business processes must be reviewed and revised through business process reengineering to maximize the use of leading commercial practices and minimize the customization of adopted commercial business systems.[52] This legislation aims to ensure that DBSs are interoperable, efficient, and aligned with DoD's strategic objectives. However, the ownership of defense business processes by their respective functional leads at DoD and service levels has led to systems that are primarily designed to meet the needs of their specific communities rather than fostering broader interoperability.

The DBEA was established to guide stakeholders toward the implementation of interoperable DBSs, but the DBEA's focus has primarily been limited to defining IT system requirements and compliance. This shift reflects the bias of the "law of the instrument," where an organization primarily focused on IT system management tends to favor IT solutions for business challenges that might be better addressed through process reengineering or organizational redesign. This behavior is further reinforced by the perception of other executives and senior leaders that the CIO serves a technical role focused on maintaining digital infrastructure rather than contributing strategically to top level decisionmaking.[53]

The current DBEA defines DoD's common E2E business processes at a high level, ensuring consistency in terminology, structure, and objectives. Although this consistency is critical for meeting the goals of reducing redundancy and improving interoperability, process owners have reported challenges in aligning their unique operational needs to the common framework. As noted in the 2024 Planning, Programming, Budgeting, and Execution (PPBE) Reform Commission report, "Many business processes are not fully understood and nor supported from an end-to-end (e.g., procure-to-pay; hire-to-retire) perspective which requires sharing information and data across organizations and systems that are often not integrated across the Department."[54] These challenges highlight the need for flexibility and adaptive implementation strategies to address the diverse process-oriented requirements of subordinate organizations while maintaining alignment with overarching mandates.

Our analysis of the DBEA and its implementation related to the alignment and reengineering of defense business processes reveals several challenges and opportunities for improvement. Although the DBEA provides a foundational framework for standardizing E2E business processes, its overwhelming focus on IT system solutions and the limited strategic role of CIO hinders its effectiveness in addressing broader enterprise needs. Misalignment between top-down mandates and bottom-up implementations, coupled with communication gaps across organizational levels, create inefficiencies and barriers to achieving interoperability. These findings highlight the need for a more holistic approach to process reengineering, strategic leadership, and adaptive implementation strategies across the DoD business enterprise.

---

[52] U.S. Code, Title 10, Section 2222.

[53] Anthony B. Gerth and Joe Peppard, "The Dynamics of CIO Derailment: How CIOs Come Undone and How to Avoid It," *Business Horizons*, Vol. 59, No. 1, January–February 2016.

[54] Commission on Planning, Programming, Budgeting, and Execution Reform, *Defense Resourcing for the Future: Final Report*, March 2024, p. 237.

Challenges in DBEA Focus and CIO Role

The DBEA's focus on IT systems as solutions limits its effectiveness in addressing broader enterprise challenges, such as process reengineering, organizational redesign, and data integration. This limitation is compounded by the perception of CIO as a technical role rather than a strategic contributor. The importance of an architecture is that it helps ensure the accuracy of data used to make decisions across the broader enterprise. This underscores the need for CIO to leverage its strategic roles derived from the CCA and the Federal Information Technology Acquisition Reform Act to influence departmental strategies.

Challenges in Process Alignment

While the DBEA provides a common framework for E2E business processes, some process owners have struggled to align their unique operational needs with this framework. For example, processes such as procure-to-pay and hire-to-retire require sharing information and data across organizations and systems that are often not integrated across the department.[55] One interviewee noted that while the DBEA represents the department's general operations, it is up to the services to ensure that lower level processes reflect reality and comply with LRPs that sometimes mandate outcomes and sometimes are much more specific regarding tasks, activities, and system constraints.[56] This misalignment can result in gaps in meeting operational needs, reinforcing the viewpoint that automation should be secondary to ensuring that processes are fit for purpose.

Communication and Implementation Challenges

At each level of the enterprise, decisions and interpretations lead to branching in the design and implementation of DBEA-relevant activities. Breaks in communication occur in both top-down and bottom-up directions, creating unique challenges for each organization. Without centralized awareness, these challenges are replicated across business functions and services. For example, top-down mandates often lack the flexibility needed for adaptive or evolutionary implementations, while bottom-up adaptations may fail to fully satisfy the intended purpose of the mandate. This dynamic underscores the need for a more integrated approach to communication and implementation across the enterprise. While the recent shift to a new federated DBEA approach is intended to mitigate the lack of flexibility from a systems perspective, it does not incorporate policy, leading practices, or other guidance on the improvement of communication. Instead, CIO's documentation cites a definition of a federated approach that "enables component organization autonomy while ensuring corporate or enterprise-wide linkages and alignment where appropriate,"[57] a wholly systems view of

[55] "For example, the Office of the Undersecretary of Defense for Personnel and Readiness (USD(P&R)) and the United States Air Force (USAF) can both create a segment to define Human Resources. Both segments must align to the L1 E2E, but the USAF segment must also map to the OUSD(P&R) segment, as OUSD(P&R) is the Department-wide lead for Human Resources" (DoD, 2024a).

[56] DoD officials, interviews with the authors, September 2024 through April 2025.

[57] DoD, 2024a.

interorganizational interactions. One interviewee noted that the ambiguity in defining what constitutes a business system, regardless of the existence of a formal definition, has led to inconsistencies in alignment with both the established frameworks of the DBEA and the DODAF. This lack of clarity complicates the integration of various IT systems, necessitating legal consultations to achieve consensus on system classifications and undermining the intended coherence of the federated architecture.[58] It reveals a gap in the guidance's effectiveness regarding communication and developing a shared understanding among stakeholders.

Compliance with Applicable Laws

Financial statement auditability goals are closely tied to the need to comply with applicable law and produce high-quality business and financial information—two of the goals of the DBEA, as stated in Title 10, Section 2222.[59] The DBEA maps OAs and information systems to applicable LRPs to help ensure compliance. Although financial statement audit covers only a subset of the LRPs included in the DBEA, it is the only DoD business activity included as one of the 17 areas shielded from reductions in the current defense budget.[60] Financial statement auditability is a good indicator of DoD's broader compliance with laws related to business systems, processes, and financial reporting—key objectives of the DBEA.[61]

DoD efforts to obtain a successful financial statement audit were once tied closely to DBEA efforts. Levine notes that DBEA efforts began in the early 2000s when a DoD commission identified the hundreds of outdated, non-interoperable business information systems as a root cause of the department's financial disarray.[62] Similarly, the PPBE Reform Commission assessment on "Financial Management Systems and Their Relationship to Financial Auditability" views the DBEA as one of the "organizational initiatives . . . implemented in the name of business systems transformation" to enable adoption of COTS technology and a successful financial statement audit.[63] There is also substantial overlap in the DBEA's E2E business processes and the E2E business processes used to classify material weaknesses in DoD financial audits since 2011 (see Table 3.1).[64]

[58] DoD officials, interviews with the authors, September 2024 through April 2025.

[59] Section 2222 directs the BEA to enable DoD to "comply with all applicable law, including Federal accounting, financial management, and reporting requirements" (U.S. Code, Title 10, Section 2222, (e)(3)(B)). Financial audits place a similar requirement on management, though focused on financial reporting: "DoD management is responsible for complying with provisions of applicable laws, regulations, contracts, and grant agreements related to financial reporting." See DoD, *Agency Financial Report: Fiscal Year 2024*, 2024c.

[60] Aaron Mehta and Ashley Roque, "Pentagon Seeks to Shift $50B in Planned Funding to New Priorities in FY26," *Breaking Defense*, February 19, 2025.

[61] Several experts challenge the value of financial statement auditability for the Pentagon (see Levine, 2020; Hanks, 2005). We do not provide any opinion on whether financial statement auditability is a worthy goal; we recognize that it is directed by law.

[62] Levine, 2020, pp. 149–223.

[63] Commission on Planning, Programming, Budgeting, and Execution Reform, 2024, pp. 230, 232.

[64] Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Financial Improvement and Audit Readiness (FIAR) Guidance*, U.S. Department of Defense, April 2017, pp. 64–65.

Table 3.1. Overlap in E2E Business Processes in BEA and DoD Financial Statement Audit Efforts

E2Es Only in BEA	E2Es in Both BEA and Financial Statement Audit
Concept-to-Product (C2P)	Acquire-to-Retire (A2R)—Equipment
Cost Management (CM)	Acquire-to-Retire (A2R)—Real Property
Deployment-to-Redeployment Retrograde (D2RR)	Budget-to-Report (B2R)
Environmental Liabilities (EL)	Hire-to-Retire (H2R)
Excess-to-Disposal (E2D)	Order-to-Cash (O2C)
Market-to-Prospect (M2P)	Plan-to-Stock (P2S)
Proposal-to-Reward (P2R)	Procure-to-Pay (P2P)
Request-to-Delivery (R2D)	
Service Request-to-Resolution (SR2S)	
Service-to-Satisfaction (S2S)	

SOURCES: Features information from DoD, 2024a, pp. 8–11; and Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, 2017, pp. 64–65.

Initial Financial Improvement and Audit Readiness Efforts Aimed to Leverage the BEA, But It Is No Longer Central to These Efforts

DoD began its Financial Improvement and Audit Readiness (FIAR) efforts in 2005 to prepare for a financial statement audit. We reviewed historic FIAR guidance documents to understand how FIAR guidance incorporated the DBEA. In the original 2005 FIAR guidance, the DBEA was clearly viewed as a tool for managing changes in financial information systems and processes to ensure auditability. For example, the initial FIAR guidance issued in 2005 required that "all system solutions must align with the Business Enterprise Architecture"[65] and emphasized FIAR's integration with the DBEA, which provides "a uniform framework and facilitates continuity in systems and process improvements."[66] Furthermore, most of the FIAR efforts described in the guidance included a section describing how those efforts integrated with DBEA efforts.

Although the frequency with which the DBEA was mentioned in FIAR guidance generally declined after the initial guidance, it reached its pinnacle of integration in the March 2008 FIAR plan. That plan describes how its E2E business process framework adapted "process steps and activities" from the DBEA,[67] and it further outlines a value proposition from this FIAR/DBEA integration: (1) integration ensures that DBEA and FIAR efforts are working with consistent systems architectures; (2) FIAR efforts can leverage the LRPs that the DBEA documented across business processes; and (3)

[65] Office of the Under Secretary of Defense (Comptroller), *Defense Financial Improvement and Audit Readiness Plan*, U.S. Department of Defense, December 2005, p. 13.

[66] Office of the Under Secretary of Defense (Comptroller), 2005, p. 70.

[67] Office of the Under Secretary of Defense (Comptroller), *Financial Improvement and Audit Readiness Plan: FIAR Plan*, U.S. Department of Defense, March 2008.

by using the DBEA, FIAR efforts can validate its information and may identify useful areas to expand the DBEA.

As the years passed, FIAR references to the DBEA declined. The DBEA was frequently referenced in discussions of the Defense Agencies Initiative, which is an enterprise resource planning (ERP) system that was designed to achieve favorable financial audit results and comply with the DBEA. The final references to the DBEA found in FIAR reports were in the November 2017 FIAR guidance.[68] We did not identify any references in more recent FIAR reports, which have been released annually after a gap around the initial audit that occurred in 2018.

The DBEA's lack of traction in financial statement audits likely reflects a deeper issue: DoD's tendency to underestimate financial statement audit challenges and overestimate its ability to address them effectively. Previous research focusing on the Army but also looking at the other services concluded that "most large DoD organizations, including the Army, have historically underestimated financial audit challenges and under resourced financial audit remediation efforts."[69] Similarly, Levine reviewed many of the failed initiatives that have occurred throughout DoD's financial statement audit efforts and concluded that these initiatives, including the DBEA, "proved beyond the capacity of the department, producing few concrete results despite the expenditure of hundreds of millions of dollars."[70]

The DBEA could be a critical tool in achieving and sustaining a clean audit opinion. All the purposes assigned to the DBEA in Title 10, Section 2222, directly address or provide a foundation for financial statement audit success:

- **Compliance** (Title 10, Section 2222, Sec. (e)(3)(B)(i)). The DBEA should help DoD business systems comply with LRPs that are necessary for a clean audit opinion.
- **Production of high-quality financial and business information** (Title 10, Section 2222, Sec. (e)(3)(B)(ii)). The DBEA should help DoD improve the quality of its financial statements, which is necessary for a clean audit opinion.
- **Integration of business systems and integration of legacy systems into the to-be system** (Title 10, Section 2222, Sec. (e)(3)(B)(iii and iv)). Such integration guided by the DBEA would support a clean audit opinion because audit efforts would be less manually intensive and less susceptible to errors.

A prerequisite for using the DBEA to obtain and sustain a clean financial statement audit opinion is likely to be the integration of DBEA efforts into FIAR and Risk Management and Internal Control (RMIC) processes. In our discussions with DoD stakeholders, we identified little evidence that the DBEA is being used as a tool in those processes. Without this type of integration, the DBEA's

[68] The November 2017 FIAR plan discusses the BEA twice regarding actions that it was taking to comply with recommendations from a House Armed Services Committee panel: (1) The BEA was adopting new E2E processes to improve development of ERPs (p. A4-9), and (2) BEA data standards were to be used to improve data conversions when moving to a new ERP (p. A4-12). See Office of the Under Secretary of Defense (Comptroller), *Financial Improvement and Audit Readiness (FIAR) Plan Status Report*, U.S. Department of Defense, November 2017.

[69] Drake Warren, Maria McCollester, Katharina Ley Best, Frank Camm, Ryan Consaul, Sandra Kay Evans, Paul W. Mayberry, Lewis Schneider, Nathaniel Edenfield, and Sheervon Husband-Clarke, *Organizing for Army Financial Audit Success: Steering Army Organizations Toward Financial Audit Success*, RAND Corporation, RR-A2409-1, 2024, p. 9.

[70] Levine, 2020, p. 152.

development may not align with audit needs, limiting its potential to effectively guide and improve audit efforts.

The DBEA's requirement to document the as-is state of business systems could be useful in facilitating financial statement audit by showing auditors how business systems link to financial processes. Such efforts are driven by an underlying assumption that the complexity of DoD's myriad systems and processes could be mitigated by increasing auditors' familiarity with those systems and processes. As audits have identified material weaknesses and thousands of Notices of Findings and Recommendations (NFRs), the need for change has become more apparent.[71]

The DBEA could be an important tool in facilitating change efforts that are documented in the DBS audit remediation plan. The DBEA (and component-specific BEAs) have most commonly been used to support the rationalization of business systems, which is a goal of that plan. The DBEA has also been used to help guide business system modernization, which could be important as DoD replaces legacy systems with systems that are compliant with the Federal Financial Management Improvement Act (FFMIA), including ERPs.

A potential starting point for integrating the DBEA into financial statement audit efforts could be to identify ways it could help DoD efforts to remediate financial information system material weaknesses. Of the 28 material weaknesses identified by DoD's independent auditor in FY 2024, the first six concern information system controls. In most cases, these weaknesses can extend to nonfinancial business systems or even mission-related systems.

1. **Financial management systems modernization.** DoD must transform its business systems to be FFMIA compliant. Contributing to this material weakness, in the auditor's opinion, is that DoD does not "have a complete and accurate list of financial management systems." This failure suggests that DoD has failed to implement a high-quality DBEA, which should provide this visibility.[72]
2. **Configuration management.** DoD components do not have "proper configuration management controls" for system changes; therefore, "DoD increased the risk of unauthorized or inappropriate changes to the financial management systems, which may impact data reliability."[73]
3. **Security management.** DoD components do not adequately monitor financial management system security issues or make plans to mitigate.
4. **Access controls.** DoD components had several deficiencies on reviewing, approving, and removing access to financial management systems.
5. **Segregation of duties.** DoD components do not manage segregation of duties for user accounts and privileges.[74]

[71] Warren et al. describe such an example: U.S. Army Financial Management Command was initially focused on building a website called the Army Process Portal, "which documents Army business processes and can be used to familiarize auditors with those processes" (Warren et al., 2024, p. vii). The command's efforts have shifted toward aiding remediation efforts to solve auditor-identified problems and audit sustainment efforts to ensure that risk-mitigation efforts remain effective.

[72] DoD, 2024c, p. 78.

[73] DoD, 2024c, p. 79.

[74] DoD, 2024c, pp. 81–84.

6. **Interface controls.** DoD components do not comply with requirements for "controls over the timely, accurate, and complete exchange of information between systems and applications on an ongoing basis, and complete and accurate migration of clean data during conversion."[75]

[75] DoD, 2024c, p. 86.

Chapter 4

Applicable Lessons from Other Organizations

Applicable lessons from analogous architecture frameworks used by foreign governments and industry provide insight into how DoD could augment existing practices to more effectively achieve the objectives of the DBEA. We structured our review of alternatives to the DBEA into two components: public (government-developed) frameworks and architectures and private (industry-led) frameworks and architectures. While our analysis makes this distinction, the road to a successful enterprise architecture is often path agnostic, as hybrid approaches provide both the flexibility of industry agility and the bedrock of government-standardized meta-models.

Enterprise Architecture Alternatives: International Partners and Allies

Our review of international analogs to the DBEA focused primarily on the FVEY security partnership, which includes the United States, the UK, Australia, Canada, and New Zealand. The FVEY relationship represents one of our most robust military-to-military information sharing partnerships. Consequently, there is a high degree of enterprise architecture similarity between these countries and frequent knowledge-sharing of the meta-models themselves and enterprise architecture best practices. Additionally, there is high alignment of the FVEY enterprise architectures to both defense and business mission sets.

UK Analogs

The UK has undergone significant transformation in enterprise architecture over the last three decades, reflecting both shifts in technology maturity and public sector priorities. In recent years, the UK government has prioritized a focus on developing a strategic reference architecture to improve data sharing and intragovernmental interoperability, improve modernization of data management, and develop reusable business capabilities and digital products. These modernization efforts include such coordinating modular component architectures as the technical reference architecture, the data reference architecture, and the business reference architecture.[76] Respectively, these reference architectures ensure (1) clear definitions and implementation of underlying technologies, infrastructure, hardware, software, networks, and security protocols; (2) consistent data governance,

[76] Jack Hanson, "The Strategic Architecture Behind Our Digital Future," *DWP Digital* blog, August 11, 2022.

information exchange, and common meta-models to enable secure and interoperable information sharing; and (3) complementary business process modernization across siloed departments, providing a structured blueprint for how activities and functions are delivered. Other guidance from the UK government has been promulgated to address the maturity of these reference architectures and has provided best practices on how to enable better intragovernmental communication of relevant data.[77] The development of the UK's enterprise architecture across the public sector and defense and the relevant defense meta-models are of particular interest because of their similarity to the DBEA. Two such examples stand out for the UK.

UK Reference Architecture

Within the last ten years, the UK government resolved to create an agreed-upon set of proven EA structures and common vocabulary, defining the critical elements that compose the UK government's information and communications technologies (ICT) landscape. In 2012, the UK government received feedback from various stakeholders to assess the robustness of its current strategy. The UK Reference Architecture (UKRA) study's purpose was to standardize public sector ICT, in a whole-of-government approach, to define common language and components for business applications and their data. The study reviewed the U.S. Federal Enterprise Architecture Framework (FEAF) and the Australian Government Architecture (AGA) framework models, agreeing that the UKRA should adopt a similar approach.[78] Although the UKRA was not fully implemented in a single framework, that document laid critical groundwork for modernizing the architecture practices across the UK government, likely influencing such subsequent initiatives as the Data Standards Authority (2020) and the application programming interface (API)-driven reference architectures (2021). The UKRA study found several lessons relevant to federated enterprise architectures, as shown in Table 4.1.

Through UKRA, the civilian UK government adoption of enterprise architecture has been focused on providing interoperable services across components, requiring continuous evaluation and engagement from stakeholders. Similarly, the EA development in the UK Ministry of Defence (MoD) has focused on implementing strategies that break down siloed practices and streamline relationships within the MoD, extending to allies and North Atlantic Treaty Organization (NATO) partners.

UK Ministry of Defence Architecture Framework

Along with ontological frameworks for integrating government services using EA, development of military architecture frameworks and meta-models within the UK's MoD have also been positioned to enable interoperability with partner nations. Historically, the UK Ministry of Defence Architecture Framework (MODAF) has mirrored and subsequently diverged from the U.S. DODAF.[79] Organized into seven standardized views (e.g., strategic, operational, systems) to capture different organizational perspectives, MODAF emphasizes visualization of complex systems through diagrams (e.g., AV-1,

[77] UK Government Digital Service and Central Digital and Data Office, "Develop Your Data and APIs Using a Reference Architecture," webpage, March 22, 2021.

[78] HM Revenue and Customs, *UK Government Reference Architecture: Government ICT Strategy*, January 2012.

[79] Matthew Hause, Graham Bleakley, and Aurelijus Morkevicius, "Technology Update on the Unified Architecture Framework (UAF)," *INCOSE International Symposium*, Vol. 26, No. 1, July 2016.

OV-1) and a unified data model.[80] These military architecture frameworks provide the standardization necessary to develop and define consistent modeling practices or "views" for an organized defense EA.[81] The development of MODAF since its introduction has consequently gone through iterative development, culminating in the withdrawal of MODAF formally in the MoD in favor of a more internationally minded and interoperable architecture framework, the NATO Architecture Framework (NAF). The crossover and iterative development of MODAF, DODAF, NAF, and the Canadian Department of National Defence Architecture Framework (DNDAF) are visualized in Figure 4.1.

Table 4.1. UKRA Lessons Learned

Key Lesson	Description
Common vocabulary and reference models	Inconsistent terminology and underused business and data reference models have caused fissures between organizations, which prevent effective collaboration and streamlining of practices, leading to siloed systems and duplicated efforts.
Stakeholder consensus	Active "buy-in" or consensus and early, continuous, and committed stakeholder engagement are required to ensure proper adoption and EA relevance. This process may result in winners and losers, but a consistent whole-of-government approach has distinct advantages in both resource allocation and scaling technologies in support of target architecture development, business process reengineering, and mission fulfilment.
Responsible governance	UKRA called for a central governance body to maintain, update, and enforce the architecture.
Efficiency is modularity	UKRA advocated breaking down processes and systems into modular, reusable components with interoperable APIs.
Open standards	Open standards lower the barriers to entry for EA providers, foster innovation, and make integrating updated technologies efficient.
Continuous evolution	UKRA recognized the dynamic nature of the ICT landscape, in which architectures continually need to be reviewed and refined.
International benchmarking	The UKRA study demonstrates the value of crowdsourcing best practices from the U.S. FEAF and Australia's AGA to enhance the development of the UK's reference architectures.

SOURCE: Features information from HM Revenue and Customs, 2012.

MODAF and its meta-model evolution (the MODAF Meta-Model, which evolved into the MODAF Ontological Data Exchange Mechanism) provide critical lessons surrounding the development, implementation, and successful evolution of defense enterprise architecture. While MODAF initially kept compatibility with the core DODAF viewpoints, subsequent iterations included differences, such as the strategic and acquisition viewpoints.[82] Over time, these semantic differences in ontological structure and component relationships created the need for standardization

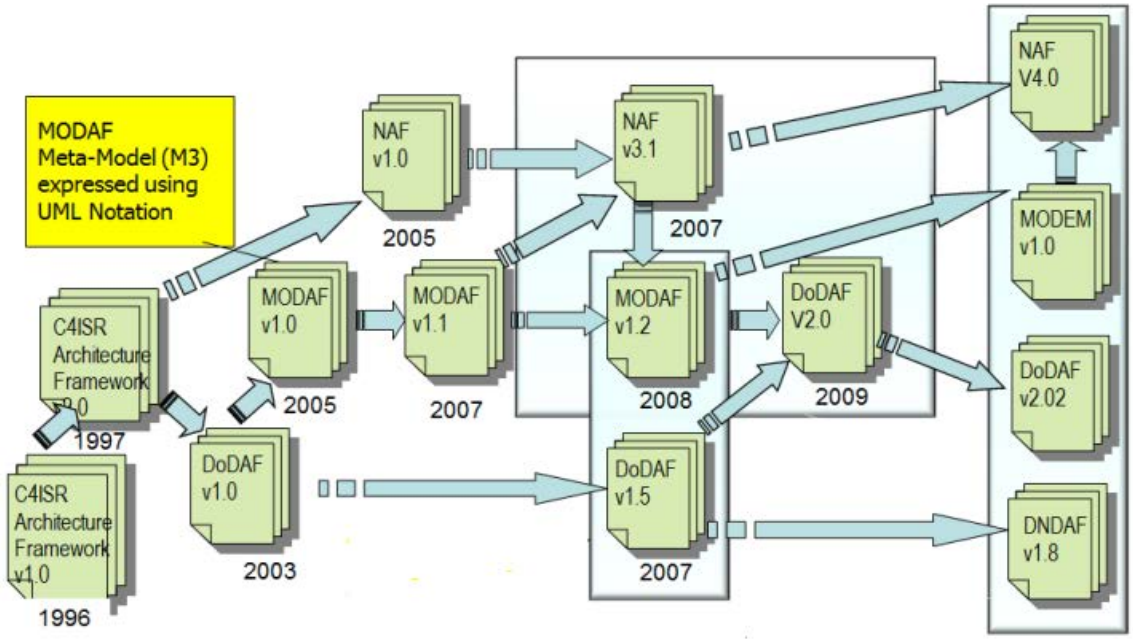
[80] Government of the United Kingdom, "Guidance: MOD Architecture Framework," webpage, last updated August 7, 2020.

[81] Hause, Bleakley, and Morkevicius, 2016.

[82] Hause, Bleakley, and Morkevicius, 2016.

in ontological modeling practices. This standardization was developed through the International Defence Enterprise Architecture Specification for Exchange Group in 2015 and through a transition of MODAF to a consolidated NAF version 4 (NAFv4) in January 2021.[83] Despite the withdrawal of MODAF in favor of the more interoperable NAFv4, the UK's defense architecture framework remains influential in legacy systems. Moreover, its development provides evidence that (1) strong technical reference models are the cornerstone of interoperability in EA; (2) centralizing EA approaches require common meta-model definitions and vocabulary to ensure proper understanding of transferred information; and (3) continual evaluation of an architecture's utility, and consequently the architecture's evolution to meet the demands of the mission, are vital to supporting stakeholders in their policy decisionmaking.

Figure 4.1. Defense Architecture Framework Iterations



SOURCE: Adapted from Hause, Bleakley, and Morkevicius, 2016, Figure 1.
NOTE: C4ISR = command, control, communications, computers, intelligence, surveillance, and reconnaissance; MODEM = MODAF ontological data exchange mechanism.

Canadian Analogs

Defence Enterprise Architecture Programme

The 2001 Defence Planning Guidance, subsequent establishment of the Director of Enterprise Architecture within the Assistant Deputy Minister for Information Management, and creation of the Department of National Defence (DND)/Canadian Armed Forces (CAF) Enterprise Architecture

[83] Government of the United Kingdom, 2020.

Programme (EAP) codified the push for enterprise architecture adoption in the CAF.[84] The initial DND EAP, structured as a federated model, focused on three main areas: EA development, EA management, and EA client support.[85] These early measures enabled all DND/CAF organizations to develop and employ a standard architecture framework, DNDAF, and a software tool for integrating information across the CAF. However, it was not until 2008 that EA, through DNDAF, was promulgated as Canadian Forces General Message (CANFORGEN) 017/08.[86] Moreover, in the same way that the U.S. DBEA is meant to facilitate a holistic understanding of the defense enterprise for senior decisionmakers, the EAP also served as a unique repository of information for greater transparency, broader dissemination, and understanding across the DND/CAF enterprise.[87] Other enduring features of the EAP include (1) decision support for planning; (2) target architectures to assist with process reengineering; and (3) EA tools, training (e.g., helpdesk, SME assistance), and resources for supporting EA activities.[88]

Overall, the DND EAP demonstrates that when properly implemented and integrated into a function of strategic management, EA can become a powerful enabler of information transparency and organizational alignment and can provide the necessary evidence for data-driven decisionmaking. However, challenges remain for the DND EAP. Issues with the EAP's maturity include a lack of cultural acceptance throughout the workforce and from senior leadership as to the effectiveness of EA, lack of direction and development of internal plans for architecture maintenance, misalignment of performance metrics to desired EA outcomes, and siloed EA support within independent level 1 organizations.[89]

Department of National Defence and Canadian Forces Architecture Framework

Because of its close value alignment with the overarching DND EAP, DNDAF provides the necessary guideposts for enterprise architecture in the CAF. Under the 2008 CANFORGEN 017/08 guidance, DNDAF was to be used across all architecture activities to ensure a holistic platform for decisionmakers—unlike the historically siloed, dispersed, and non-shareable frameworks, models, and tools used throughout the CAF.[90] The architecture consists of "eight architectural views (common, strategic, capability, operational, system, technical, information and security) and their associated sub-views."[91] However, DNDAF's architectural taxonomy has been criticized for not providing a

[84] J. K. Stewart, "A Case for Enterprise Architecture in Department of National Defence Strategic Management," Canadian Forces College, Canadian Armed Forces, 2016.

[85] Stewart, 2016.

[86] Department of National Defence, *Promulgation of the Department of National Defence and Canadian Forces Architecture Framework (DNDAF) and the Defence Architecture Data Model (DADM)*, Government of Canada, January 2008.

[87] Stewart, 2016.

[88] Stewart, 2016.

[89] Stewart, 2016.

[90] Stewart, 2016.

[91] Stewart, 2016.

comprehensive methodology to integrate the architectural components into an accurate representation of the enterprise.[92]

While DNDAF was heralded as one of the most advanced military architecture frameworks upon release in 2008—compared with DODAF, MODAF, and other frameworks—it was not perceived as comprehensive enough and needed to address a number of shortcomings and limitations.[93] One limitation presented is the degree to which DNDAF accurately and completely represents the enterprise. As an example, one assessment found that "it is likely that DNDAF products are not optimized to meet the needs of the Royal Canadian Navy decision-makers, and as supported by academic research, it is likely that a comprehensive DNDAF EA would be costly to develop and maintain."[94] Unlike DODAF's six-step architecture development process, DNDAF initially lacked a formalized process for developing architectural descriptions and focused on using the Microsoft Office suite of tools while working to identify an acceptable EA toolset.[95] Despite federated implementation of DNDAF, where each level 1 organization is responsible for implementing frameworks and tools in alignment with DNDAF guidelines, fragmentation of architectural priorities and use is commonplace.

Critical lessons from the development of the EAP and DNDAF include the following:

- The EAP requires a strong mandate to compel organizations within defense to capture and manage their architectures as they begin to adapt to changing requirements.
- The purpose of DNDAF should be to support strategic-level decisionmaking and the collective goals of the department and ensure that a methodology that can address the challenges of all stakeholders is adequately provided.
- Securing buy-in from relevant stakeholders, leveraging talent and training personnel on DNDAF, and building a system to support EA management ensures effectiveness.
- Providing adequate training and guidance on EA's use cases and clearly articulating what EA cannot do is vital to ensuring that the tool is used properly and with due regard and compliance with relevant governance.

Australian Analogs

Australia's first embrace of enterprise architecture began with the introduction of the Defence Architecture Framework (DAF, later the Australian Defence Architecture Framework 2 [AUSDAF2]) to the Australian Department of Defence circa 2003.[96] The DAF was initially composed of blueprints, derived from DODAF, containing specific technical information and visual

[92] R. Farahbod, A. Guitouni, and E. Bossé, *Towards a Comprehensive DND/CF Enterprise Architecture Methodology: A Critical Review DNDAF for an Integrated C2 Capability Development*, Defence Research and Development Canada, June 2013.

[93] Farahbod, Guitouni, and Bossé, 2013.

[94] T. B. Gibel, "Steadying the Course: Enterprise Architecture in the RCN," Canadian Forces College, Canadian Armed Forces, 2015.

[95] Farahbod, Guitouni, and Bossé, 2013.

[96] Meredith Hue, "A Review of Enterprise Architecture Use in Defence," Department of Defence, Australian Government, September 2014b.

diagrams for architecture artifacts, designed to be a solution-agnostic approach to EA.[97] Although other countries, such as the United States and UK, prescribed their respective DODAF and MODAF architectures with unique domain meta-models and vocabularies, the DAF allows users the flexibility of choosing either or both DODAF and MODAF artifacts, unconstrained by semantic distinctions between them.[98] This architecture evolved to become AUSDAF2, to support the development of the notional Integrated Defence Architecture (IDA). In its second iteration, the AUSDAF2 chose to reorganize and included similar artifacts to DODAF, excluding a unique defined meta-model, such as the DODAF Meta-Model.[99] A depiction of the evolution of the DAF, AUSDAF2, and AGA is shown in Figure 4.2.

Integrated Defence Architecture

Australia's IDA is a comprehensive framework designed to align defense capabilities, business processes, and technology investments across its Department of Defence. In its first iteration, the IDA focused on defining the business architecture—documenting "the business strategy, governance, organization, and key business processes information, as well as the interactions between these concepts."[100] The IDA also employs multiple reference models and organizes architectural views (operational, systems, and technical), similar to DODAF 2.0. Overall, the IDA was meant to provide decisionmaking support, guide EA development, and ensure consistent use of architecture frameworks, such as the AUSDAF2.

However, in a holistic review of the Australian defense EA practices, the IDA's guidance has been criticized as fragmented, leading to a reliance on disparate third party sources and institutional knowledge rather than robust internal guidance and standards.[101] As of 2014, the architecture lacked sufficient formal methods to account for production of architectural information, such as data storage practices, and lacked service-related requirements, and stakeholders lacked the perceived resources to support the development and demands of the IDA.[102] Overreliance on contractors, lack of formal training materials, and lack of robust re-skilling courses for the existing workforce have also significantly impacted retention of corporate memory.[103] This has resulted in broad integration and IDA development challenges when applied beyond enterprise-wide activities and has sown doubt from stakeholders as to the utility of EA in achieving the goals required of the department.

[97] Hue, 2014b.

[98] Meredith Hue, "An Analysis of SE and MBSE Concepts to Support Defence Capability Acquisition," Department of Defence, Australian Government, September 2014a.

[99] Hue, 2014a.

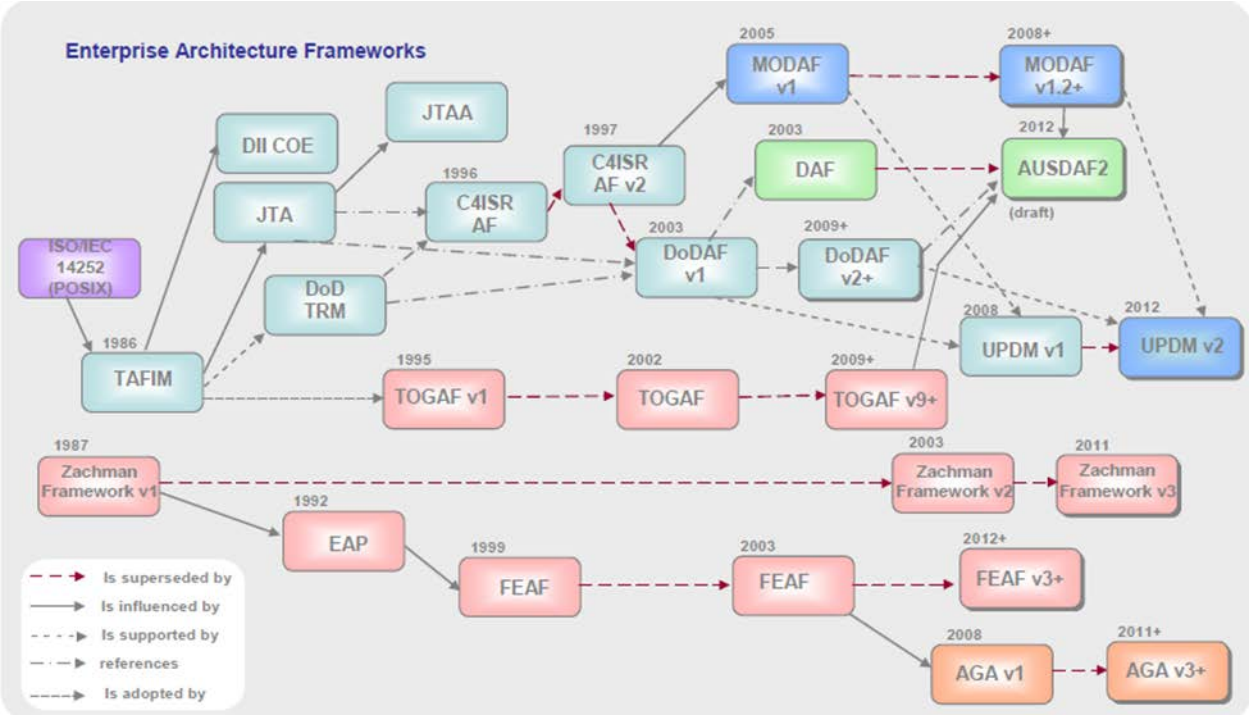
[100] Hue, 2014a.

[101] Hue, 2014b.

[102] Hue, 2014b.

[103] Hue, 2014b.

Figure 4.2. Australian Architecture Evolution



SOURCE: Reproduced from Hue, 2014a, p. 71, Figure 29.
NOTE: AF = architecture framework; COE = common operating environment; IEC = International Electrotechnical Commission; ISO = International Organization for Standardization; TOGAF = The Open Group Architecture Framework; TRM = Technical Reference Model; UPDM = Unified Profile for DoDAF and MODAF.

Defence Business Reference Architecture

In September 2015, the Associate Secretary (Chief Operating Officer) assembled a focus group to address perceived inadequacies of available reference architectures within the senior echelons of the Australian government.[104] The proposed model, the Defence Business Reference Architecture (DBRA), is a capabilities-based approach, agnostic of both delivery method and organization, developed to map out the relationships and interdependencies among the major elements within the Australian Department of Defence.[105] By focusing on capabilities, the DBRA provides a structured approach to understand how various business processes and technology components contribute to defense objectives, without creating unnecessary duplication of effort across departments or being too closely aligned to one organization, and focusing on the output to senior leadership, rather than on the technical specifics of the model itself.[106] Overall, the DBRA acts to provide context to support operational tasking, supports the implementation of new service models, and assists with business process mapping and reengineering.[107]

[104] Department of Defence, "Defence Business Reference Architecture," briefing slides, Australian Government, 2015.

[105] Department of Defence, 2015.

[106] Department of Defence, 2015.

[107] Department of Defence, 2015.

Australian Government Architecture

After an independent review in 2008 concerning the necessity of government to provide a common framework to develop ICT infrastructure,[108] the Australian Government Information Management Office within the Department of Finance and Deregulation created and enforced the adoption of reference models, which together represent the AGA.[109] The AGA provides "a centralized, whole-of-government framework which supports digital transformation across civilian government agencies by providing a shared resource of digital artifacts, policies, standards, and design guidance."[110] As an EA, the AGA is based on the FEAF developed by the United States.[111] The AGA is organized through five reference models: performance, business, service, data, and technical.

These reference models act to provide a consistent framework for addressing concerns across multiple government agencies and mapping out capabilities, policies, and standards for each agency, ensuring consistency in architecture approach and alignment of digital investments in ICT development.[112] The AGA is accessible to all agencies and the public, promoting standardization and reuse of architecture products across government. Agencies are not required to replace their existing architectures with the AGA; however, those that do not have an existing architecture are encouraged to review the AGA when planning new investments,[113] and alignment is assessed through the Digital and ICT Investment Oversight Framework. The AGA's library of artifacts is designed to reduce siloed decisionmaking and foster a whole-of-government approach to digital capability delivery. However, the AGA has faced criticism regarding inadequate governance and a lack of ongoing improvement processes, which can limit its effectiveness in practice.

Key insights emerge from the different architectures and models described within the purview of the Australian government:

- A perception exists around EA in the Australian government, particularly the AGA model, of inadequate governance and lack of process to continually improve the models—making the use of these models ineffective.
- Fragmented guidance on IDA practices left the Department of Defence significantly reliant on cross-referencing with disparate third parties instead of internally communicating.
- The IDA lacks formalisms that consider the second- and third-order effects of process implementation, such as the physical and threat environments.
- Utilizing the IDA for non-enterprise-wide activities leads to significant integration problems because of the lack of robustness in replacing established practices.

---

[108] Peter Gershon, *Review of the Australian Government's Use of Information and Communication Technology*, Australian Government Information Management Office, August 2008.

[109] Hue, 2014b.

[110] Australian Government, "Australian Government Architecture," webpage, undated.

[111] Department of Finance and Deregulation, *Australian Government Architecture Reference Models*, Australian Government, August 2011.

[112] Australian Government, undated.

[113] Australian Government, undated.

New Zealand Analogs

Government Enterprise Architecture for New Zealand

Similar to the UKRA and the AGA, the Government Enterprise Architecture for New Zealand (GEA-NZ) is a whole-of-government framework designed to provide a common language and categorization that promotes consistency in government business processes, services, and infrastructure.[114] The GEA-NZ, refreshed in 2021, is structured around eight top-level dimensions:[115]

- strategy, investment, and policy
- governance and performance
- standards
- business
- data and information
- application and ICT services
- infrastructure
- security and privacy.

Earlier iterations of the GEA-NZ focused on enabling four key outcomes: success of government goals and objectives, functional integration, authoritative reference, and resource optimization.[116] Its major components—business, data/information/analytics, application/software services, and infrastructure—provide agencies with a consistent approach to modeling and managing their processes, assets, and capabilities.[117]

The framework is mandated for use across the public sector to enable agency alignment of enterprise architectures with government-wide strategic goals, ensure that process development is cost effective, and support ICT-enabled transformation and collaborative cross-agency projects.[118] Unlike other frameworks that have received much international attention and independent investigation, the GEA-NZ is still constantly evolving to meet the demands of the New Zealand government. Current work is still underway in the New Zealand government, through the Government Enterprise Architecture Group, to redevelop the GEA-NZ, calling the replacement the GEA-NZ 2024 Framework.[119]

NATO Analog

NAFv4 Architecture Framework

Fundamentally, successful implementation of enterprise architecture relies on system interoperability and trust, between both internal and external stakeholders. Moreover, the architecture

[114] New Zealand Government, "Enterprise Architecture," webpage, undated.

[115] New Zealand Government, "About the GEA-NZ Framework," webpage, last updated February 10, 2025.

[116] New Zealand Government, *Government Enterprise Architecture*, June 2015.

[117] New Zealand Government, "Overview of the GEA-NZ Framework," webpage, last updated March 1, 2021.

[118] New Zealand Government, 2015.

[119] New Zealand Government, "Redevelopment of the GEA-NZ Framework," webpage, last updated November 21, 2024.

frameworks—those that provide common foundation of ontological principles, definitions, and data structures—are the bedrock that enables a comprehensive and interoperable enterprise architecture. Previously discussed architecture frameworks, such as MODAF and DODAF, have provided a strong precedent for the utility of such technical reference architectures. However, while DODAF remains the standard architecture for the U.S. DoD, other partner nations within NATO—the UK, France, and Germany—have collaborated to realize NAF as an enduring standard for EA.[120]

The unique contribution that undergirds the effectiveness of NAF, now in its fourth iteration, is the centrality of its architecture management plan. Through the architecture management plan, the NAF prioritizes interoperability through a host of measures, such as benchmarking international policy and standards and adoption of commercial models and frameworks. Focusing on military and business system integration through iteratively updated dashboards, the NAF ensures data consistency, traceability, and transparency to all international stakeholders through the use of various internationally recognized standards (e.g., the Institute of Electrical and Electronics Engineers, International Organization for Standardization/International Electrotechnical Commission).[121]

In addition, NAFv4 references Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H, CJCSI 6212.01F, and DoD Instruction 4630.08, incorporating the lessons learned from the U.S. challenges with interoperability, development of DODAF, and the Joint Capabilities Integration and Development System (JCIDS) process to inform and improve on the characteristics of the architecture framework.[122] Interestingly, the NAFv4 takes inspiration from DODAF's six-step architecture process and extends it to encompass migration plans for both a new architecture reference model and candidate target architectures while ensuring compliance with enterprise portfolio priorities.[123] This mapping is pictured in the NAFv4 document and provided in Figure 4.3.

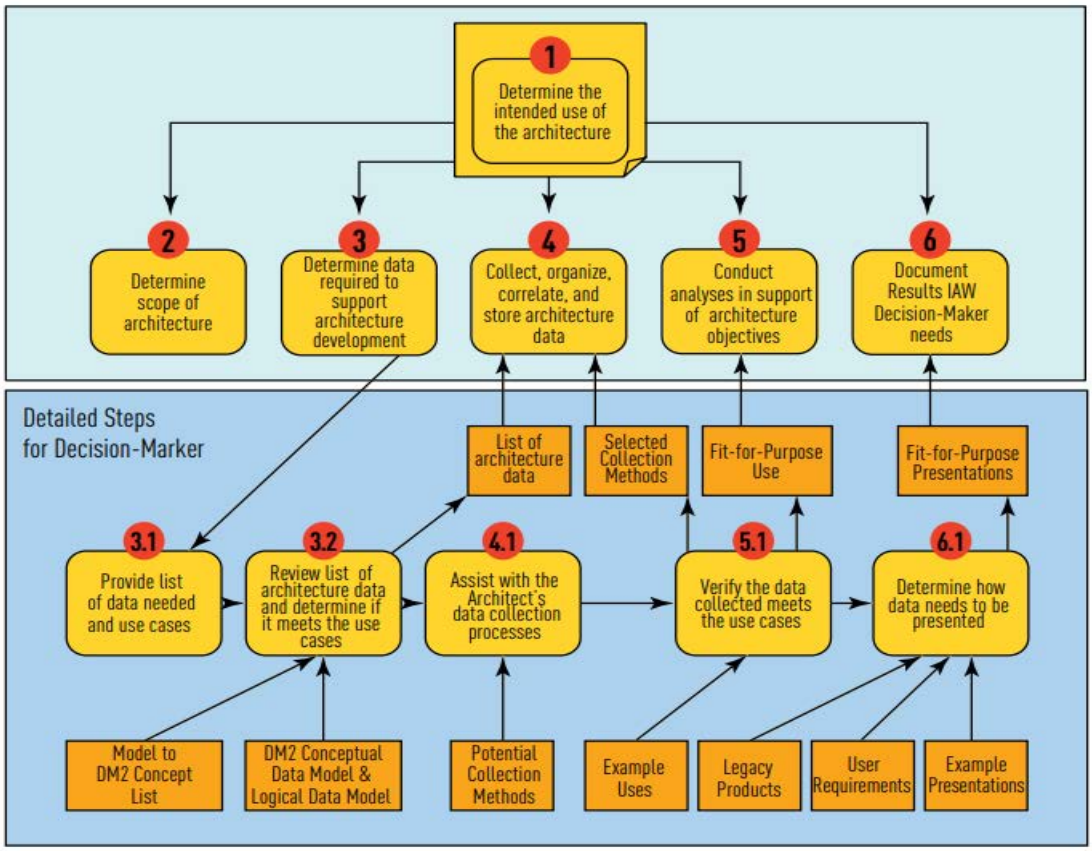
[120] Architecture Capability Team, *NATO Architecture Framework*, Consultation, Command & Control Board, North Atlantic Treaty Organization, September 2020.

[121] Architecture Capability Team, 2020.

[122] Architecture Capability Team, 2020.

[123] Architecture Capability Team, 2020.

Figure 4.3. DODAF Six-Step with NAFv4 Extension



SOURCE: Reproduced from Architecture Capability Team, 2020, Figure 2-12, p. 42.

Furthermore, NAFv4 incorporates not only the perspectives of NATO member architectures but also those that are commercially available. For example, the methodology unpinning NAFv4 is inspired by The Open Group Architecture Framework (TOGAF)/Architecture Development Method (ADM) version 9.1, with an improvement to the requirements management stage, allowing for more traceable architecture products.[124] Of the common vocabulary incorporated in NAFv4, 17 out of 54 terms are adapted from TOGAF.[125] NAFv4 also uses the UAF meta-model, as well as the open and independent modeling language, Archimate, as its acting meta-models to standardize viewpoints.[126]

The integration of perspectives from government architectures, such as DODAF; best practices and pitfall mitigation strategies; and adoption of the commercial TOGAF framework, UAF, and accompanying Archimate modeling language demonstrate the hybrid value of NAFv4.[127] By crowdsourcing the best modularized components for this architecture, NAFv4 stands as an exemplar

[124] Architecture Capability Team, 2020; *The TOGAF Standard*, Version 9.1, Van Haren Publishing, 2011.

[125] Architecture Capability Team, 2020.

[126] Architecture Capability Team, 2020.

[127] Architecture Capability Team, 2020.

framework for expanding the value proposition of EA for public-sector use, creating an EA that truly is more than the sum of its parts.

Allied Nations Lessons Learned

Various examples from the FVEY nations and NAF show the distinct benefits and drawbacks of using enterprise architecture as a panacea (Table 4.2). Successful enterprise architecture is often developed slowly, involves many stakeholder discussions and feedback, and, above all, relies on common procedures and thoughtful definitions. While EA is not a one-size-fits-all approach, utilizing the lessons learned from the FVEY nations provides necessary context and a blueprint for avoiding pitfalls and embracing organizational change when developing enterprise architecture.

Table 4.2. Allied Nations Overarching Lessons Learned

Key Lesson	Description
Stakeholder engagement and consensus-building	Securing ownership and buy-in from all stakeholders is crucial for successful adoption of any EA. Deliberate EA strategies, which seek feedback on how to craft the right architecture for the problem and under what circumstances, must achieve consensus and garner commitment across diverse departments to enable an EA that simultaneously meets the demands of the mission while providing traceability and transparency for all stakeholders.
Dynamic and evolving framework	Reference architectures are not static, nor should they be. EAs require continuous updates and improvements to deliver on their value proposition. These updates should consider the EA operating domain and conditions, the practices of other reference models (commercial and government), and the workforce that will be using the EA. This requires that the EA authority implement mechanisms for ongoing review and integration of evolving EA standards and definitions. Successful EA programs must require a sustainable, scalable, and repeatable process for gathering and documenting organizational information. An effective EA must evolve to meet the current and future needs of stakeholders while factoring in organizational changes, strategic direction, and transformation initiatives.
Robust governance to prevent "shelfware" (i.e., technical debt)	Effective governance is essential to ensure that the architecture remains relevant and utilized for its intended purpose. Establishing reference architectures provides a blueprint for further EA development but does not equate to consistent and effective architecture management. Lines of responsibility must be articulated clearly to ensure that architectures are properly instantiated and maintained. Developing methods of collaboration and engagement across EA consumers is therefore essential to supporting effective governance models and OAs.
Disparity in EA practice	Notable inconsistencies in the understanding and application of EA, with different interpretations of its purpose and methodology across defense organizations, have led to inefficiencies and misaligned efforts. Establishing clear guidelines for the scope, applicability, and limitations of EA practices should ensure that EAs are aligned to their intended purpose and scope. Utilizing a centralized meta-model with defined management guidance provides the most organizational transparency to an EA, enabling interoperability through consistent vocabulary, relationship structures, and relevant constraints levied on artifacts and relationships within the EA.
Reliance on individuals	Guidance on EA policy often heavily relies on the institutional knowledge of individuals rather than structured documentation. When changeover occurs, the EA workforce may experience difficulty adapting to the high learning curve. To ensure workforce knowledge-sharing and best practices, organizations should establish standardized procedural guidance that should evolve with the EA. These structured practices create clear methodologies in architectural practices and underpin information exchange within the architecture.
Fragmentation and lack of formality	The absence of explicit linkages between various EA initiatives and a formalized methodological approach leads to ineffective EAs. Organizations should invest in developing a workforce skilled in EA and provide access to relevant training and tools to facilitate EA reform and process reengineering.

SOURCES: Features information from HM Revenue and Customs, 2012; Hue, 2014b; and Stewart, 2016.

Enterprise Architecture Alternatives: Private Sector and Industry

The analysis of private-sector alternatives and models for the DBEA focused on identifying the state-of-the-art processes, frameworks, and meta-models used across a variety of large commercial organizations. We conducted a landscape overview of the most commonly used EA approaches across the industry, as well as the best practices imbued by the frameworks, meta-models, and methods of combining these tools for an integrated approach with the respective models in DoD.

The Evolution and Strategic Role of Enterprise Architecture

Enterprise architecture has evolved significantly in recent years, driven by the adoption of agile and lean methodologies that emphasize iterative development, continuous delivery, and adaptability. Traditional EA approaches, often criticized for their rigidity and slow responsiveness, struggled to remain relevant in dynamic business environments. Modern frameworks have addressed these limitations, enabling organizations to align architectural practices with rapidly changing requirements and foster innovation in enterprise planning and execution.[128] This transformation has made EA more responsive to real-time business needs, positioning it as a critical enabler of organizational agility and resilience.

The integration of such emerging technologies as AI, ML, cloud computing, and blockchain has further revolutionized the role of EA. These technologies empower organizations to automate processes, analyze large scale data, and enhance decisionmaking capabilities, thereby establishing EA as a strategic driver of digital transformation.[129] Industry leaders are also leveraging advanced tools and platforms, such as ArchiMate, TOGAF, LeanIX, and Sparx Systems Enterprise Architect, to streamline visualization, modeling, and collaboration. These tools make EA more actionable and accessible across diverse teams, reinforcing its role in driving organizational success.[130] Furthermore, EA has shifted from IT-centric objectives to a focus on measurable business outcomes, such as revenue growth, improved customer experience, and operational efficiency.[131] Decentralized and federated approaches are also gaining traction, enabling individual business units to collaborate and contribute to EA frameworks. This collaborative model fosters innovation and ensures that EA evolves in alignment with diverse organizational needs, making it a dynamic and adaptable tool for modern enterprises.[132]

---

[128] Jeanne W. Ross, Peter Weill, and David C. Robertson, *Enterprise Architecture as Strategy: Creating a Foundation for Business Execution*, Harvard Business School Press, 2006.

[129] *The TOGAF Standard*, Version 9.3, Van Haren Publishing, 2023; George Westerman, Didier Bonnet, and Andrew McAfee, *Leading Digital: Turning Technology into Business Transformation*, Harvard Business Review Press, 2014.

[130] Marc M. Lankhorst, Henderick Alex Proper, and Henk Jonkers, "The Architecture of the ArchiMate Language," paper presented at 14th International Conference on Exploring Modeling Methods in Systems Analysis and Design, 2009; *The TOGAF Standard*, Version 9.2, The Open Group, 2021.

[131] Marc Lankhorst, *Enterprise Architecture at Work: Modeling, Communication and Analysis*, Springer, 2017; Ross, Weill, and Robertson, 2006.

[132] *The TOGAF Standard*, 2023; Ross, Weill, and Robertson, 2006.

Industry Lessons Learned

Industry has revolutionized enterprise architecture by making it more agile, business-focused, and technology-driven.[133] Governments have incorporated EA to enhance public service delivery, optimize costs, and drive digital transformation.[134] While challenges remain, the growing convergence between industry innovation and government adoption signals a promising future for EA as a strategic tool across sectors.

Table 4.3 summarizes different industry approaches, including benefits, challenges, and use cases of the frameworks we reviewed.

[133] Ross, Weill, and Robertson, 2006; Frederik Ahlemann, Eric Stettiner, Marcus Messerschmidt, and Christine Legner, eds., *Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments*, Springer, 2012.

[134] U.S. Office of Management and Budget, *Federal Enterprise Architecture Framework (FEAF)*, 2012.

Table 4.3. Industry Alternatives: EA Frameworks

Category	TOGAF	Zachman	Gartner
Model approach	Structured methodology (ADM) to align IT with business goals, supported by reusable assets, predefined templates (e.g., Technical Reference Model, Integrated Information Infrastructure Reference Model), and strong governance and compliance focus	A taxonomy organized as a two-dimensional matrix with six perspectives (rows: executive, business management, architect, engineer, technician, and enterprise) and six questions (columns: what, how, where, who, when, and why)	Business-driven approach aligning IT with business strategy and outcomes, centered on six key elements: business outcomes, strategy, information, technology, people, and processes
Benefits	Standardized, scalable framework providing a common language for architects, aligning IT with business goals, and promoting asset reuse across industries	Flexible taxonomy with a comprehensive scope, offering a holistic view of enterprise interdependencies and improving communication across industries and technologies	Flexible and adaptable framework prioritizing business outcomes, fostering collaboration between IT and business leaders, and leveraging emerging technologies for transformation
Drawbacks	Complex for newcomers, requiring skilled personnel, significant time for implementation, and customization to meet specific industry needs	Taxonomy-based framework that is abstract, challenging for smaller organizations, and requires complementary methodologies for practical implementation	Lacks a prescriptive methodology, requiring skilled practitioners for effective adaptation, and may overlook detailed technical aspects compared to TOGAF
Use cases	Supports digital transformation by aligning IT with business goals, modernizing legacy systems, and ensuring regulatory compliance	Facilitates structured documentation, system integration by identifying gaps, and risk assessment through analysis of dependencies and vulnerabilities	Drives digital transformation by integrating technology, aligns IT with strategic business goals, and supports cloud adoption while maintaining business alignment

SOURCES: Features information from *The TOGAF Standard*, 2023; Aurona Gerber, Pierre le Roux, Carike Kearney, and Alta van der Merwe, "The Zachman Framework for Enterprise Architecture: An Explanatory IS Theory," *Responsible Design, Implementation and Use of Information Communication Technology*, I3E 2020, *Lecture Notes in Computer Science*, Vol. 12066, April 1, 2020; Amazon AWS, "AWS Well-Architected," webpage, undated-d; Google Cloud, "Google Cloud Well-Architected Framework," webpage, last reviewed October 11, 2024; Microsoft Learn, "Microsoft Cloud Adoption Framework for Azure," webpage, undated-c; SAP Learning, "Enterprise Architect," webpage, undated; Gartner, "Build Your Enterprise Architecture Discipline," webpage, undated.

Comparative Takeaways from Industry EA

Enterprise architecture frameworks face challenges related to resistance to change, complexity, and skills gaps. TOGAF, Zachman, and Gartner each address these issues differently, with varying levels

of prescriptiveness, accessibility, and focus on implementation guidance. Table 4.4 highlights some of the key challenges for each of the enterprise architecture frameworks.

Table 4.4. Challenges for EA Frameworks

Challenge	TOGAF	Zachman	Gartner
Resistance to change	Resistance arises from its complexity and IT-centric perception, with pushback from nontechnical stakeholders struggling to align EA with broader business goals	Resistance stems from its less prescriptive nature, requiring significant customization, while its rigid structure and unfamiliar terminology can alienate stakeholders	Accessible to nontechnical stakeholders, but perceived focus on strategic goals over operational details can cause resistance
Complexity	The highly detailed ADM can overwhelm organizations with limited EA experience and poses challenges for large-scale implementation without substantial resources and expertise	Focus on classification over process complicates the management of large-scale architectures and lacks implementation guidance	Reduces complexity with actionable insights, but scaling across large organizations is challenging due to varying stakeholder expectations
Skills gap	Requires specialized knowledge of ADM and tools like ArchiMate, limiting adoption due to a shortage of trained professionals	Requires a deep understanding of taxonomy and classification, which can intimidate newcomers, while the lack of process guidance worsens the skills gap	Mitigates skills gap by emphasizing collaboration and outcomes over technical expertise, but lack of standardized training programs poses challenges

SOURCES: Features information from *The TOGAF Standard*, 2023; Gerber et al., 2020; Gartner, undated; Amazon AWS, undated-d; Google Cloud, 2024; Microsoft Learn, undated-c; SAP Learning, undated.

Nevertheless, enterprise architecture frameworks also offer opportunities for innovation, global collaboration, and scalability. TOGAF, Zachman, and Gartner each provide distinct approaches, leveraging emerging technologies, fostering interoperability, and addressing scalability through modular, taxonomic, or outcome-driven methods. Table 4.5 highlights some of the key opportunities for each of the enterprise architecture frameworks.

Key Takeaways

Our review highlighted strengths of various industry approaches. TOGAF's modularity allows organizations to experiment with innovative solutions without disrupting the entire architecture. Its widespread adoption enhances compatibility with other organizations using the same framework, and its structured approach advances consistency across diverse teams and geographies. For Zachman, its flexibility may enable organizations to incorporate emerging technologies without rigid process constraints, and its classification system seeks to enable organizations to align their architectures conceptually across borders. The Zachman taxonomy supports scalability by accommodating diverse

perspectives and domains. In contrast, Gartner offers a focus on actionable insights, which can accelerate the deployment of innovative solutions. Its iterative approach claims to foster cooperation by emphasizing shared value creation, and its agility promotes scalability without overwhelming stakeholders.

Table 4.5. Opportunities for EA Frameworks

Opportunity	TOGAF	Zachman	Gartner
Innovation	Iterative ADM integrates emerging technologies like AI, cloud computing, and blockchain into architectural design.	Structured taxonomy facilitates integration of new technologies across perspectives (e.g., business, data, technology).	Agile, outcome-focused approach encourages experimentation and rapid adoption of emerging technologies.
Global collaboration	Standardized approach supports interoperability and collaboration across multinational organizations and governments.	Universal taxonomy provides a common language for collaboration but lacks process guidance for practical implementation.	Flexible and outcome-driven framework aligns diverse goals, promoting adaptability in global contexts.
Scalability	Modular ADM supports scalability by focusing on specific phases or domains, but scaling requires significant resources.	Classification system is inherently scalable but lacks guidance for implementing scalable processes.	Iterative approach prioritizes high-impact areas, enabling incremental expansion and scalability.

SOURCES: Features information from *The TOGAF Standard*, 2023; Gerber et al., 2020; Gartner, undated; Amazon AWS, undated-d; Google Cloud, 2024; Microsoft Learn, undated-c; SAP Learning, undated.

Chapter 5

Findings and Recommendations

Section 922 of the FY 2024 NDAA directs an assessment of the DBEA as of the date of the enactment of that act. As we began this study, the DBEA was being reconstituted under CIO leadership and could best be described as a partially populated framework that would itself be expected to change as it matures. As a federated construct, the DBEA includes individual segments of varying levels of maturity. In this assessment, we considered the capability of the DBEA to support defense business operations across the department, noting that all E2E processes involve multiple services and other DoD components and almost all cross functional boundaries as well.

Finding 1. DoD CIO's new federated architecture framework is a promising approach, but institutional inertia and a lack of compelling use cases have the potential to stall its momentum.

From its origins and as encoded in Section 2222(e), the DBEA has always been an uneasy hybrid of business architecture and enterprise architecture. As a business architecture, the DBEA is intended to help leadership modernize and perform defense business operations more efficiently while meeting emerging needs. This business view is supported by the DBEA's traditional subordination to the CMO and the DBC and its core standards of E2E processes and OA hierarchy models mapped to LRPs. As an enterprise architecture, the DBEA is intended to enforce technical standards, support system rationalization, and help modernize the department's information systems. The nature of most of the legal specifications and the core mapping of business systems with the OAs, E2Es, and LRPs support the enterprise architecture view of the DBEA. The dissolution of the office of the DoD CMO and placement of the DBEA under the control of DoD CIO shifted the balance toward an enterprise architecture approach—an enterprise architecture for DBSs rather than a business architecture that additionally addresses information systems—leaving in place the centerpiece standards of the E2Es, OAs, LRPs, and DBC ownership. As a result, the new DBEA framework is still not clearly aligned toward optimal use as either a business architecture or an enterprise architecture.

Architecture helps to identify problems or strengths of the current state and to plot a path toward a new state, but it is only meaningful if the beginning state reflects reality and if the transformations projected are legitimate and feasible. In several respects, the DBEA models a reality that did not exist in practice. A notable example is the process through which systems are required to assert compliance with the DBEA annually for release of funds. This process gives the appearance that the certification authority is the decisionmaker, but in practice, most systems are owned, funded, and controlled by service functionals rather than the certification authority. Note that this does not imply that members of the DBC are not important decisionmakers in their own right; it just reflects the fact that neither the structure of the DBEA nor the certification process effectively changes their responsibilities. Interviewees reported that some business processes do not map accurately to the established E2Es or to processes represented by OAs, lending another aspect of incorrect modeling. Interviewees also reported that it is common for system owners to assert compliance to the DBEA even when they meet

only a fraction of the requirements of the associated LRPs. Lacking an accurate starting model of essential features, an enterprise architecture cannot realize its potential to support analysis of issues, projections of a different end state, and development of a feasible path to the end state.

The new federated DBEA approach established in January 2024 addresses some of these problems but does not overcome them completely. It acknowledges the distributed responsibilities of the department and does not try to force a picture of unified decisionmaking. It incorporates a modified set of centrally managed E2Es, LRPs, and catalog of approved OAs but also outlines a process for services and agencies to work with OSD functional leads in developing and modifying those artifacts to meet current and new business needs. The new DBEA approach states the intention to be data-driven and questions-based, but we did not find any active use cases other than supporting the annual certification process in the same manner as the previous DBEA. Use cases can come from any source, but without them—without questions that need to be asked and the data, analytics, and visualizations to answer them—the new DBEA reverts to being the centerpiece of a compliance exercise only.

Recommendation 1a. The DBC should define initial use cases to address bounded problems necessary to prepare for financial statement audit.

In 2023, DoD CIO and the Under Secretary of Defense (Comptroller) collaborated on a proof-of-concept activity intended to inform and demonstrate the value proposition of the new DBEA approach. Beyond a demonstration, the DBC needs to identify its first use cases and move forward with leveraging the DBEA. Characteristics of a good use case include that the problems addressed are within the decision space of the organization sponsoring it; it is bounded in scope such that the decisionmaker can expect to see results within their remaining tenure; and the value to the organization of those results can be assessed through meaningful strategic metrics.

We see financial statement audit as an opportunity-rich space within which to identify and pursue initial DBEA use cases. Financial statement audit is regarded by leadership throughout the department with urgency, and many of the material weaknesses identified by independent auditors involve business system mapping and controls. We recommend that DoD explore one or more efforts like the following:

- an effort led by CIO and the Under Secretary of Defense (Comptroller) to rationalize financial systems in the defense and field agencies, similar to the current Army enterprise architecture-informed methodology or the Navy's Cattle Drive
- (any) agency-led effort to identify systems and data needed for its next audit produced in a format useful for presentation to an independent audit agency
- a CIO-led effort to identify and address shortcomings in audit-relevant system controls for defense and field agency systems, such as those identified in the first six material weaknesses listed in the 2024 DoD agency financial report.[135]

Recommendation 1b. DoD CIO should form a partnership with CDAO to better enlist the Advana enterprise data and analytics environment in realizing the DBEA's full potential.

[135] DoD, 2024c.

The strength of a DBEA is in its ability to answer questions. Currently and in the near term, people will continue to go to the DBEA to comply with legislation; they will continue to go to Advana when they have questions to answer. Rather than try to preemptively rebrand the DBEA into a tool to answer questions rather than a tool to assert compliance, DoD CIO and CDAO should jointly ensure that Advana supports a streamlined, coherent process that draws on—and helps maintain—DBEA structure and information resources in the service of business operations and management decisions. Advana is listed among the resources involved with the DBEA; we recommend a shift such that Advana becomes more of the face, and engine, of the DBEA.

Finding 2. The DBEA requires greater flexibility and stakeholder engagement to fulfill its purposes with respect to defense business systems and business process reengineering.

Many interviewees indicated that they felt "boxed in" when interacting with the DBEA. There were several aspects to this perception. The structure of the DBEA, including its use of DODAF reference models, is perceived as inflexible and ill suited to more modern aspects of the DBS environment. These newer and emerging aspects include the use of nontraditional information systems (such as a SharePoint site or data lake) for sharing or transforming business data and the use of more modern software development capabilities, such as agile methodologies, generative AI, and the software acquisition pathway. Like the previous DBEA (BEA 11.2), the new version has not yet reconciled the tension between top-down mandates and the needs of the system owners and developers. Some interviewees indicated that the standardized E2Es and OAs used in the assertion and certification processes do not match their systems' actual business processes. The new DBEA framework promises flexibility that will be necessary to overcome these challenges and keep pace with changing technologies, priorities, and business needs, but we have not seen any mechanisms enacted to provide that flexibility.

Recommendation 2a. DoD CIO should provide an experimentation space—a "sandbox"—to support flexibility for functional and mission alignment.

The new DBEA approach promises greater flexibility, but the mechanisms for ensuring that flexibility are not elaborated. In many ways, DoD business operations reflect webbed responsibilities rather than clear, undisputed hierarchical relationships. Title 10 of the U.S. Code gives service secretaries responsibilities for business operations and the systems that support them. The Secretary of Defense acts through the OSD staff and also through service secretaries and combatant commanders in essentially parallel paths. Additionally, almost all the E2E processes cross organizational boundaries such that no one area of OSD or service staff is fully responsible for the entire process.[136] DBEA mechanisms should support collaboration and communication over the illusion of centralized directive control while providing common access to authoritative data and the ability to share local manipulation and reporting.

One way to enhance communication and collaboration is to provide an experimentation space to test constructs that do not conform to existing standards. Where the experimental construct proves

[136] Even for the E2E that is most cleanly aligned to a single staff element—Hire-to-Retire—the department's experience with the failed development of the Defense Integrated Military Human Resources System points to a lack of effective central authority. See Julie Pechacek, Alan Gelder, Amrit Romana, Ethan Novak, Kathy Conley, Cheryl Green, Dina Eliezer, P. M. Picucci, George Kennedy, and Cullen Roberts, *Considerations for Implementing a Defense Personnel Research Environment*, Institute for Defense Analyses, September 2018.

superior to the current standard, DBEA managers can then determine a way to implement it in the least disruptive manner. This structure could prevent picking "winners and losers," isolate areas of technical obsolescence, and promote a collaborative method for reaching consensus on the state of the art in EA.

Recommendation 2b. DoD CIO should use the experimentation space to explore potential contributions from alternative models and frameworks.

Industry and partner nation experience shows a benefit to an open standards approach to enterprise architecture, but there is immense potential for disruption in the prospect of wholesale adoption of a new framework. DoD should give itself room to try different architectures in limited cases and to test semantic logic or constructs from those architectures to answer particular needs. For example, as shown in Appendix D, the Army currently uses the Gartner LEAD model (limited, enterprise, aging, divest; see Figure D.1) as a visualization tool to help prioritize modernization efforts. The Zachman framework, with its emphasis on stakeholder interests, could provide a useful model to identify decisionmakers and incentives for various groups as an early stage of prosecuting a DBEA use case. Also, TOGAF's ADM could inform the development of DBEA use cases.

Recommendation 2c. DoD CIO should partner with DoD organizations, including the Defense Digital Service and Defense Innovation Unit, for active outreach to industry.

The department should include continuing outreach efforts to industry partners to benefit from market-driven advances in areas of enterprise architecture relevant to an ERP system. Such outreach supports the intent of the language in Title 10, Section 2222(e)(3), in using the DBEA to make effective use of industry's investments and innovation.

Finding 3. Some of the legal specifications for the DBEA are overbroad and unhelpful.

Several of the legal specifications describing the DBEA and its use act as barriers to a focused and effective application of the framework. Title 10, Section 2222(e)(3), mandates that the DBEA will "include policies, procedures, business data standards, business performance measures, and business information requirements that apply uniformly throughout the department" and enable the department to "comply with all applicable law, including Federal accounting, financial management, and reporting requirements," a practically unbounded scope.[137] Additionally, the definition of an enterprise architecture in Title 44, Section 3601(4), includes a baseline or "as-is" architecture, a target or "to-be" architecture, and a sequenced path between the two states.[138] This construct mimics an outdated waterfall acquisition approach, and several interviewees implied that they felt compelled to document the current state completely before potentially addressing change in even a narrow area. Also, it is not clear in which architectural state a law with unmet provisions would be included: the "as-is" state because the law exists, or the "to-be" state once systems and processes are developed to comply with the law.

Relative to the mandated use of the DBEA, Section 2222(g) requires that "For any fiscal year in which funds are expended for development or sustainment pursuant to a covered defense business system program, the appropriate approval official shall review the system and certify, certify with conditions, or decline to certify, as the case may be, that it continues to satisfy the requirement . . . that

[137] Public Law 107-314, 2022; Public Law 108-375, 2004.

[138] U.S. Code, Title 44, Section 3601(4).

the system and business system portfolio are or will be in compliance with the defense business enterprise architecture developed pursuant to subsection (e) or will be in compliance as a result of modifications planned." However, it does not say what it means to be "compliant" with the DBEA. These initial and annual certification processes are resource-intensive and have been demonstrably ineffective as a forcing function to promote modernization of DBSs or processes.[139] They also fail to support agile development processes and can prove a disincentive to modernization in that changed systems must use resources to remap and recertify their compliance.

Recommendation 3. The DBC should redesign the annual certification process to be meaningful and publish clear guidance for its execution.

The DBC needs to determine what they want from the certification processes specified in Section 2222(g) and redesign that process for validity and effect. In terms of validity, the DBC should state what it means to "comply" with the DBEA and not force or allow owners of covered business systems to make assertions contrary to fact. One aspect to consider is whether the centrally maintained E2Es and catalog of OAs are thought to have directive force. LRPs are directive, but the fact that E2Es or OAs map to LRPs does not give those constructs directive force. Instead, E2Es and OAs should be considered tools for communication and collaboration among the many process and system stakeholders. The DBC needs to provide clear guidance on how to reflect a system's state of compliance with DBEA artifacts, and it should also provide the tools with which to accurately show their state of compliance.

In redesigning the certification process, the DBC should consider the authorities that its members have to enact change beyond the potential of withholding execution year funds and integrate such mechanisms into the new process. There are likely to be several more useful touchpoints in the requirements process, defense acquisition system, and the PPBE system that together are more effective in achieving the goals of the certification process.[140]

Finding 4. The new DBEA needs to mature through practical application before it will provide an adequate and useful framework for planning, managing, and integrating business systems of the department.

The new DBEA framework has great potential for use in supporting rationalization and modernization of DBSs, but as of the time of this study, it has not made analytics, visualization tools, or mechanisms to respond to changing technologies or business needs available to stakeholders. To realize its full potential, the framework should focus on bounded use cases that enable the development and application of standardized tools and mechanisms where beneficial while maintaining flexibility to respond to changes. Appendix D describes the ABEA as a model for using an enterprise architecture-informed methodology to plan, integrate, and manage business systems for a major defense component. As the Army has shown, if managed effectively with appropriate

[139] See Defense Business Board, *The Chief Management Office of the Department of Defense: An Assessment*, DBB FY 20-01, June 1, 2020; and Levine, 2020.

[140] Suggestions for accomplishing this, though not vetted to the point of becoming recommendations, are (1) use the certification process to influence actions earlier in the PPBE cycle, such as the capability planning guidance, and (2) link to the JCIDS process such that operational needs are explicitly traced from the relevant LRP through one or more JCIDS documents to the business system that supports them.

governance, resources, and results-oriented focus, a BEA can achieve the goals intended by Title 10, Section 2222.

Recommendation 4. DoD CIO should improve outreach, automation, and modernization of the DBEA.

Specific activities to improve in the areas above include the following:

- Automate workflows to reduce manual data entry and manipulation and speed identification of nonconformance.
- Expand education and awareness outreach by engaging in bidirectional communication in support of business process reengineering efforts to close the gaps between mission objectives, business processes, and systems across the enterprise.
- Support the continuous evolution of the DBEA to reflect changes in systems engineering processes (e.g., generative AI) and ensure alignment across different life cycle stages. Update life cycle management and cybersecurity practices to accommodate modern software development methodologies, such as agile methodologies, while ensuring compliance with evolving security requirements.
- Leverage findings from automation and stakeholder engagement to develop and regularly review and update metrics useful for supporting strategic level objectives.

Finding 5. The DBEA is not realizing its potential to inform business process reengineering primarily because of an incentive structure focused on funding for information systems.

Although essential business process elements such as E2Es and OAs are maintained as centerpieces of the new federated DBEA framework, its reinvention under DoD CIO has firmed its focus on information systems. The prominent tools for effecting change are approving or withholding funding for information systems, and we found no formal incentives for business process reengineering outside the context of the information systems that support that business process. Even the name of the governance body established to support the DBC's leadership with respect to the DBEA—the DBS CFB—acknowledges an information system focus to the endeavor.

Despite this information system orientation, the DBEA's formulation of E2E processes across organizational boundaries supports cross-service and cross-agency communications and collaboration. This factor provides potential to leverage the DBEA in business process reengineering. A useful start would be to identify and address misalignments between the centralized framework approach and unique operational needs.

Recommendation 5. DoD CIO and the services should strengthen the ability of the DBEA to support business process reengineering efforts.

- Provide additional guidance to process owners to help them align their unique operational needs with the common framework. This could involve targeted training, workshops, and resources to ensure that lower level processes simultaneously reflect reality and comply with relevant LRPs. There also needs to be an ongoing component to ensure that alignment is maintained.
- Incorporate flexibilities to account for adaptive or evolutionary implementations to address the diverse needs of subordinate organizations. Allow services to tailor lower level processes to their unique operational requirements while maintaining alignment with overarching

mandates. Executors within subordinate organizations should be empowered to adapt processes while ensuring that they meet the intended purpose of top-down directives.
- Establish centralized awareness and improved communication mechanisms to address breaks in communication between top-down mandates and bottom-up implementations. This could include using standardized reporting frameworks, collaborative platforms, and experimentation space to ensure that challenges are identified and addressed in near-real-time. Strengthening communication would reduce duplicative efforts and improve interoperability across the enterprise.

In sum, the new federated DBEA, as stated in the January 2024 document and through its implementation during the period of this study,[141] offers a necessary reset of approach to managing and improving the department's business capabilities and operations. However, realizing its potential involves realizing key changes from the former model. DoD should craft its proof-of-concept use cases to show the value of the DBEA while driving the development of tools and practices. The department should also expand outreach to internal and external partners to make the DBEA relevant and effective.

[141] DoD, 2024a.

Appendix A

Section 922 of the FY 2024 NDAA

SEC. 922. INDEPENDENT ASSESSMENT OF DEFENSE BUSINESS ENTERPRISE ARCHITECTURE.

(a) In General. --The Secretary of Defense shall seek to enter into a contract or other agreement with a federally funded research and development center or a university affiliated research center to conduct an independent assessment of the defense business enterprise architecture developed under section 2222(e) of title 10, United States Code.

(b) Elements.--The assessment required by subsection (a) shall include the following elements:

(1) An assessment of the effectiveness of the defense business enterprise architecture as of the date of the enactment of this Act in providing an adequate and useful framework for planning, managing, and integrating the business systems of the Department of Defense.

(2) A comparison of the defense business enterprise architecture with similar models in use by other government agencies in the United States, foreign governments, and major commercial entities, including an assessment of any lessons from such models that might be applied to the defense business enterprise architecture.

(3) An assessment of the adequacy of the defense business enterprise architecture in informing business process reengineering and being sufficiently responsive to changes in business processes over time.

(4) An identification of any shortfalls or implementation challenges in the utility of the defense business enterprise architecture.

(5) Recommendations for replacement of the existing defense business enterprise architecture or for modifications to the existing architecture to make that architecture and the process for updating that architecture more effective and responsive to the business process needs of the Department.

(c) Interim Briefing.--Not later than April 1, 2024, the Secretary of Defense shall provide to the Committees on Armed Services of the Senate and the House of Representatives a briefing on the status of the assessment required by subsection (a).

(d) Final Report.--Not later than January 30, 2025, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on the results of the assessment required by subsection (a).

Appendix B

Interview Analysis

In this appendix, we provide an overview of our interview protocol and our qualitative interview analysis approach.

Interview Protocol

We conducted 26 semistructured interviews with SMEs across different military departments and organizations. We interviewed personnel who were stakeholders to the DBEA in some sort of capacity, such as whether they manage the DBEA or interact with the DBEA for their specific job purpose. Interviewees hailed from the military branches, DoD-wide offices, and GAO. A high level overview of interviewees' affiliations is as follows:

- Department of the Air Force
- Department of the Army
- Department of the Navy
- DoD CIO
- DoD human capital and human resource management SMEs
- DoD Office of the Under Secretary of Defense SMEs, including those in logistics and comptroller offices
- GAO
- U.S. Transportation Command.

Some interviews were follow-ups with the same interviewee from previous conversations to clarify statements that were made or to ask further questions. The interviews were conducted, recorded, and transcribed on Microsoft Teams, all with permission from the interviewees. Table B.1 outlines questions that were asked, but the wording may have slightly changed, clarifying questions may have been asked, and not all questions may have been covered in all interviews.

Table B.1. Interview Questions

Topic of Interest	Question
Participant background	1. What is your role with respect to defense business processes, systems, and the DBEA? a. Are you a contributor to the DBEA, a consumer, or both? b. Which areas addressed by the DBEA do you focus on? c. Which DoD Business Flows (L0 E2E Business Processes, L1 Process Areas, L2 Process Area Segments) is your organization linked to? d. What organizations do you work with closely or observe that work with the DBEA?
Implementation of statutory requirements	1. We are interested in how DoD approaches the statutory requirements of the DBEA, which include guiding the development of integrated business processes and interoperable business systems, and compliance with law. a. How do your organization's contributions to the DBEA help guide the development of integrated business processes within the DoD? i. Who are the primary consumers of that information? What feedback have you received? b. How do your organization's contributions to the DBEA help guide implementation of interoperable defense business systems? i. Who are the primary consumers of that information? What feedback have you received? c. The DBEA is supposed to include policies, procedures, business data standards, business performance measures, and business information requirements that uniformly apply throughout the DoD. From your work with it, where are the shortfalls? i. How mature would you say your organization's BEA is? ii. How mature would you say the DBEA is? iii. What challenges do differences between the DBEA and your organization's implementation cause? How have you overcome those challenges? e. The DBEA should align strategy with execution in business processes. Can you think of some specific instances in which the DBEA was used to help implement the National Defense Strategy or other DoD strategic documents like the FYs 22–26 Strategic Management Plan, DoD Cyber Strategy, or DoD Financial Management Strategy? 2. What steps do you take to integrate your organization's part of the DBEA into the existing information enterprise architecture (IEA)? 3. Focusing on the DBEA's role in helping the DoD comply with law, a. Have you been part of any audits in which the DBEA was used? i. What was your impression of the utility of the DBEA in that activity? b. The DoD is required to routinely produce verifiable, timely, accurate, and reliable business and financial information for management purposes; how effective is the DBEA in that activity? c. In what way does the DBEA integrate budget, accounting, and program information and systems?

Topic of Interest	Question
Utility of the BEA	1. The DBEA is supposed to be useful in guiding change throughout the entire defense business enterprise. How have you seen it used in planning, managing, integrating, modifying, and transforming the defense business enterprise? 2. What additional authorities would the DoD need for the DBEA to better perform these functions? 3. Are you aware of or have you participated in business process reengineering efforts in which the participants used the BEA as a guide? a. How effective was the DBEA in informing that activity? What would make it more effective? 4. How do defense business systems articulate their linkage to the DBEA?
Financial management and the BEA	1. What rules and/or policies existing on how the DBEA should be incorporated into financial management? a. Where is this documented? b. Has this changed over time? c. Do Independent Public Auditors ever look at the DBEA or make assessments regarding the DBEA? 2. Are there other ways that the financial management community uses the DBEA? a. Are there other ways that the financial management community could or should be using the DBEA? b. What changes to the DBEA would be needed to enable these changes? 3. How does the financial management community coordinate with the developers of the DBEA? 4. To what extent does the DBEA enable the DoD to be technologically interoperable across different branches and agile to the changing technological landscape?
BEA implementation	1. What tools or systems do you use to maintain your organization's DBEA? 2. Is the current process manually intensive, or can it automatically ingest necessary data? 3. Take us through the process of updating your organization's BEA, starting with how you know a change is needed. 4. The DoD is moving to a "federated BEA." To what extent are your roles and responsibilities associated with the federated BEA clear? 5. What modifications or changes to systems hosting the DBEA has your organization considered and/or implemented? Are further changes needed? 6. To what extent is the data in the DBEA standardized, easily accessible, and accurately represented? 7. What performance measures exist for the DBEA? What metrics exist for determining the effectiveness of DBEA's implementation? 8. What do you see as the lessons learned in the implementation of the DBEA to date? How might the new federated approach address past lessons learned? 9. What do you see as the future of your organization's BEA? What about the DBEA?

Topic of Interest	Question
BEA lessons learned and alternatives	1. Reaching into your past experience as well as what you've seen in DoD, let's talk about alternative information models (not a BEA as the DoD has implemented) that could be useful in accomplishing the Department's business goals. Are you aware of any other information models that the DoD either has or should consider using instead of the DBEA? 2. Thank you for sharing your insights. We may need to follow up with you on some points raised here later. In the meantime, is there anyone else we should talk to about this topic?

Qualitative Interview Analysis

Following the interviews, we completed a qualitative interview coding analysis to identify common themes across all of the interviews using Dedoose. In this context, a theme refers to a label that we created based on topics and ideas mentioned in the interviews. We grouped themes that share common attributes within a broader theme label. Conversely, we decomposed exceptionally broad themes—those conforming to a large number of interviewee statements—into more specific themes. The overall themes of perceptions expressed by interviewees involved challenges with the DBEA, enablers of DBEA success, suggested guidance to improve the DBEA, and interviewees' personal history. An example of a more specific theme within "challenges" is "governance or oversight," which is itself decomposed into more specific challenges involving "overall direction," "roles, responsibilities, and ownership," "support or engagement," "enforcement or accountability, and "cost of BEA." Specific themes are defined in Table B.2, presented hierarchically within their broader theme(s). It should be noted that the themes were documented based on the perceptions expressed by the interviewees and are not our direct assessments of the DBEA.

Table B.2. Interview Themes

Theme			Definition
CHALLENGES			
1	Governance or oversight		Any thoughts expressed by the interviewee that criticizes the way the DBEA is being led and overseen
	1.1	Overall direction	The perception that there is a lack of or no clear "to-be" destination outlined that can guide the DBEA forward in terms of improvement, modernization, and optimization efforts
	1.2	Roles, responsibilities, and ownership	The perception that roles and responsibilities are not clearly defined such that this lack results in disagreements over specific job roles and responsibilities, or ownership or authority is not clearly defined
	1.3	Support or engagement	The perception that there is limited or no action taken by leadership to support or engage with staff who interact with or maintain the DBEA

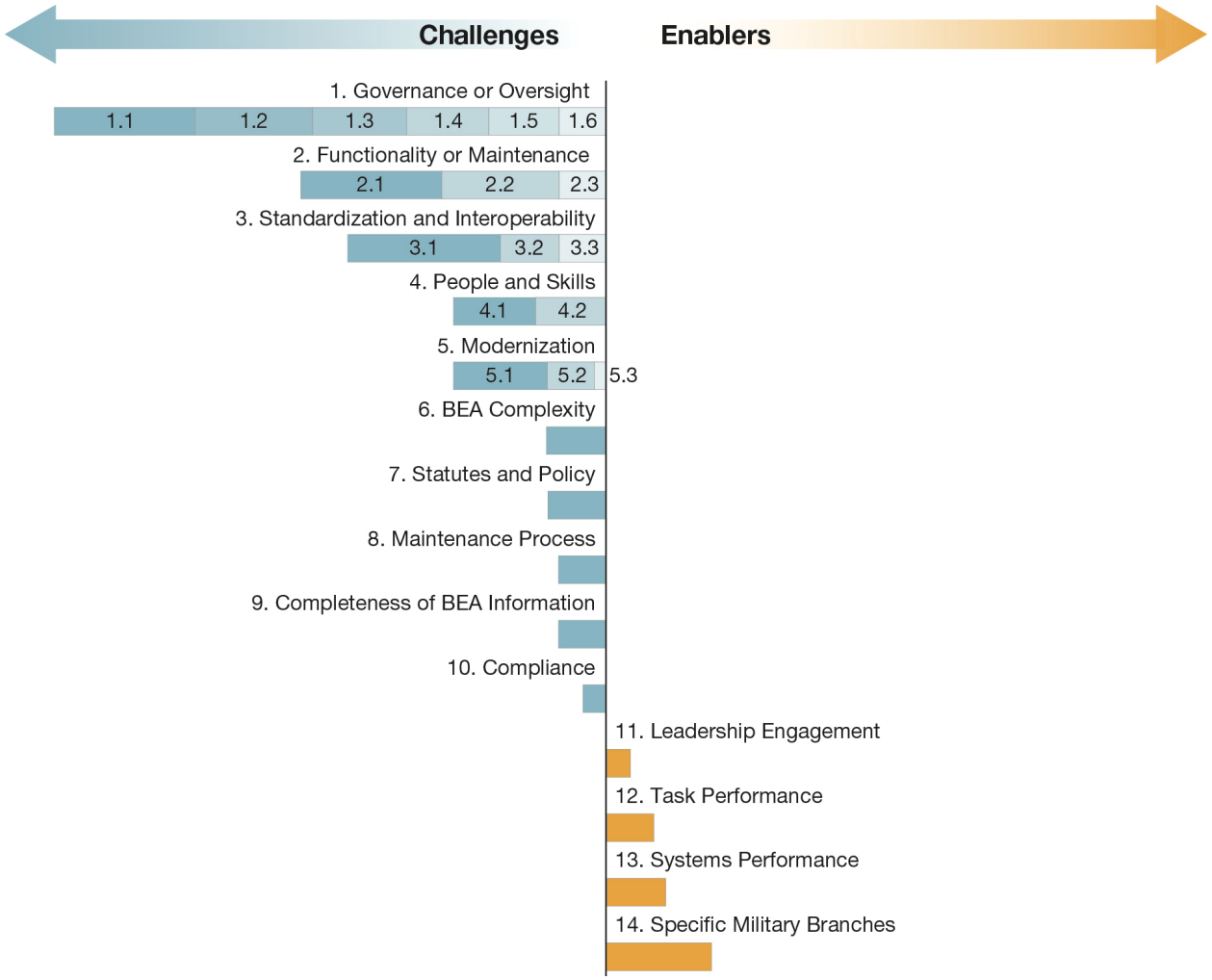
Theme		Definition
	1.4 Enforcement or accountability	The perception that there is little or no action taken by leadership against staff or organizations that do not comply with systems, policies, plans, or practices
	1.5 Cost of DBEA	The perception that an excessive amount of money was spent. While a set amount for what constitutes "high" was not made, it was implied that any mention about money spent on a system or initiative by the interviewee was viewed critically.
	1.6 Consistency in guidance	The perception that leadership would instruct for something or have the goal of doing something but then a different action would occur
2	Functionality or maintenance	Any thoughts expressed by the interviewee that the way the DBEA functions and is maintained is not sufficient to maximize its potential utility
	2.1 Picture of inventory and requirements	The perception that there is a lack of or absence of a picture of the current components and capabilities of the DBEA
	2.2 Proper use and full potential	The perception that the DBEA is not being used as originally intended, to its true intention, or in a way that its utility can be maximized
	2.3 Ability to make changes	The perception that there are roadblocks within the DBEA's infrastructure that are preventing any changes or improvements to be made
3	Standardization and interoperability	Any thoughts expressed by the interviewee that the DBEA lacks standardization and interoperability
	3.1 Decentralized practices	Perceived lack of unity in executing tasks, operational processes, or approaches, whether it be among organizations or the military branches
	3.2 Communication between groups	Perceived lack of communication among DoD organizations or military departments
	3.3 Customization	Perceived excessive customization of systems, policies, plans, or practices such there is a lack or absence of standardization or interoperability
4	People and skills	Any thoughts expressed by the interviewee that there are not enough qualified and skilled personnel needed for the DBEA
	4.1 Staffing	The perception that staffing levels do not possess the technological skills needed to maintain the DBEA
	4.2 True intention of BEA	The perception that certain personnel who interact with the DBEA have demonstrated that they are interacting with the DBEA in a way that was not originally intended
5	Modernization	Any thoughts expressed that are related to an aspect of the DBEA being outdated
	5.1 System components in the BEA	The perception that there are systems in the DBEA that need to be modernized in which their current state causes frustration from users or exacerbates ongoing problems
	5.2 Willingness to modernize	The perception that there is resistance from leadership or staff (e.g., consumers, stakeholders) of the DBEA to modernize systems, policies, plans or practices in the DBEA

Theme		Definition
	5.3 Assets in the BEA	The perception that there are outdated policies, plans, or practices in the DBEA such that they do not meet the needs of the organization
6	DBEA complexity	The perception that the DBEA has too many components such that it prevents any progress on improvement, modernization, or optimization efforts
7	Statutes and policy	The perception that the statutes or policies that dictate the DBEA are ambiguous
8	Maintenance process	The perception that there are processes or steps associated with maintaining or improving the DBEA that are manually intensive
9	Completeness of DBEA information	The perception that there is critical information, such as data, that cannot be found in the DBEA that is necessary for a staff member of the DBEA to complete their job
10	Compliance	The perception that certain actions taken that are related to the DBEA are not compliant with certain LRPs
ENABLERS		
11	Leadership engagement	The perception that leadership has been willing to engage and get involved in the process of improving or maintaining the BEA
12	Task performance	Mentions of processes that successfully perform their intended functions
13	Systems performance	Mentions of specific systems that successfully perform their intended functions
14	Specific military branches	The perception that military branches have an architecture or specific processes that perform well that the DBEA could potentially leverage
GUIDANCE TO IMPROVE THE DBEA		
	Suggested improvement for DBEA	Suggestions that were mentioned by interviewees regarding improvements that can be made to improve operations related to the DBEA
	Examples of architecture outside of DoD	Examples of architectures that were mentioned by interviewees that DoD could look to for inspiration to improve operations related to the DBEA
PERSONAL AND DBEA HISTORY		

SOURCE: Features information from DoD officials, interviews with the authors, September 2024 through April 2025.

Figure B.1 depicts the weight of themes involving challenges with the DBEA and enablers of DBEA success, as reflected by the number of interviews in which they were brought forward by interviewees. Note that this weighting does not include the number of times an individual theme was expressed in any one interview. Where broader themes are decomposed into more detailed themes, the bar in Figure B.1 sums the number of interviews within which the detailed theme was expressed. As an example, when we sum the number of interviews in which challenges with "1. Governance or Oversight" was expressed in one or more of subthemes 1.1 through 1.6, that challenge far outweighs interviewee concerns regarding "6. BEA Complexity" or the positive introduction of "Leadership Engagement" as an enabler of DBEA success.

Figure B.1. Visualizing Perceived DBEA Challenges and Enablers



SOURCE: Features information from DoD officials, interviews with the authors, September 2024 through April 2025.
NOTE: Themes and subthemes (denoted by number) are identified in Table B.2. The scale of each challenge or enabler reflects the number of interviews in which an interviewee brought up the theme.

Appendix C

DBEA Governance

The DBC is the primary senior executive departmental level governance body for the DBEA. The DBC functions to advise the Secretary on "developing the defense business enterprise architecture, reengineering the Department's business processes, developing and deploying defense business systems, and developing requirements for defense business systems."[142] The DBC possesses two chairs per Title 10, Section 2222: the DoD Performance Improvement Officer and DoD CIO. Additional members (or their designees) on the DBC include

- the CIOs of the military departments
- the CMOs of the military departments
- the Under Secretary of Defense for Acquisitions and Sustainment
- the Under Secretary of Defense (Comptroller)
- the Under Secretary of Defense for Personnel and Readiness
- the Chief Data and Artificial Intelligence Officer.[143]

The 2012 charter established that DoD CIO "develop and maintain the Defense Business Enterprise Architecture (BEA) to guide development of integrated DoD business processes."[144] Specific to the DBEA, the DBC sets priorities for DBEA development, approves changes to E2E processes at the top levels, and adjudicates intractable issues among key stakeholders.[145]

DoD CIO has also formed an executive level DBS CFB to "address rationalization and BEA requirements" and support the DBC's governance of the DBEA.[146] The DBS CFB is chaired by the Deputy CIO for Information Enterprise. According to the federated approach framework, the DBS CFB "will oversee development of BEA guidance and implementation, create requirements, assess options for the collection and visualization of BEA data (e.g., tools), and serve as the DoD BEA Configuration Control Board."[147] The DBS CFB was intended to provide input to the DBC, not supplant its oversight and direction. The DBS CFB can recommend changes in E2E processes at the top levels to the DBC and approve changes at more detailed levels of the architecture. It is also supposed to use the DBEA "to execute defense business system portfolio management objectives."[148]

[142] U.S. Code, Title 10, Section 2222.

[143] U.S. Code, Title 10, Section 2222.

[144] DoD, *Defense Business Council Charter*, 2012, p. 3.

[145] DoD, 2024b, p. 10.

[146] DoD, 2024a, p. 7.

[147] DoD, 2024a, p. 7.

[148] DoD, 2024b, p. 10.

An action officer level DBEA WG was established in March 2024 to facilitate the modernization of the DBEA. It was tasked with aligning the DBEA with the vision outlined in the federated approach to include coordination across all key stakeholders to identify and populate the DBEA with data and information across the various architectural levels. E2E process champions across the DBEA's functional areas were empowered to stand up their own coordination groups to facilitate progress with DBEA modernization.

Appendix D

The ABEA

The scope and context of the ABEA make it a useful comparative to the DBEA. The ABEA can be described as the organized set of analytics, visualizations, and underlying data used by the Army for decisionmaking in its management of business operations. The ABEA derives its structure, contents, and meaning from its use: supporting decisionmakers in managing business operations.

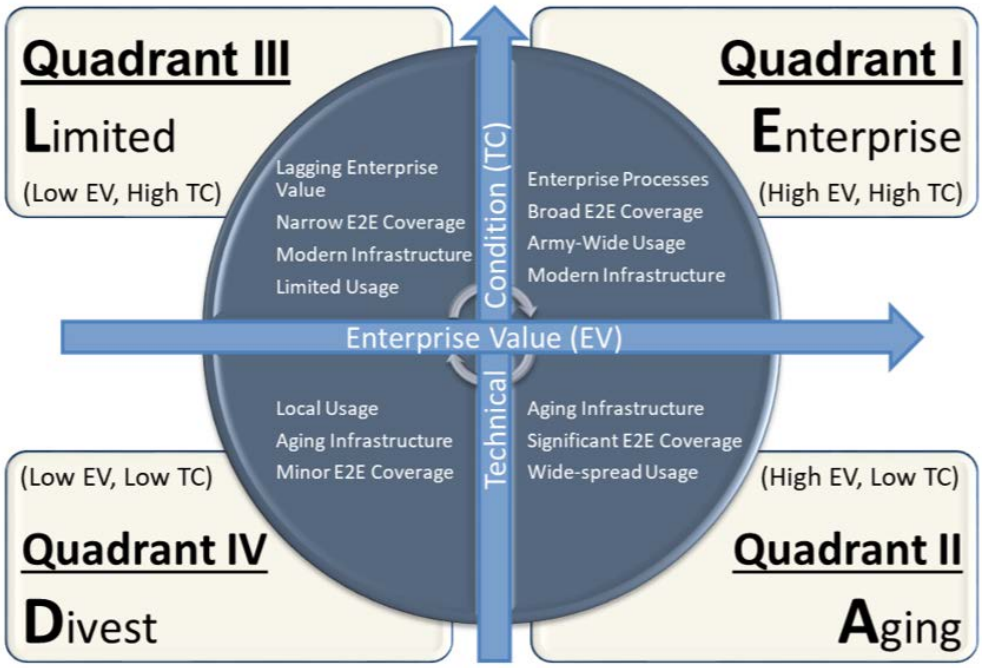
Army Regulation 5-1, Management of Army Business Operations, lays out authorities and responsibilities for staff principals, commands, and organizations involved in Army business operations, which is expansively defined as "those activities that enable the Army to execute effectively and efficiently its [Title 10, U.S. Code] primary functions to organize, man, train, equip, and sustain forces."[149] The regulation acknowledges the appointment of the Under Secretary of the Army as the department's CMO, establishing his or her authorities with respect to the development and sustainment of business processes and systems. Army Regulation 5-1 directs the development and maintenance of the ABEA and places it under the control of the Office of Business Transformation (later renamed to the Office of Enterprise Management [OEM]). According to an interviewee familiar with the organizational dynamics of the Army staff, the OEM functioned as "the Office of the CMO," with corresponding influence over business systems and processes for the department as a whole.

According to people interviewed for this study, it took several years from the publication of the November 2015 version of Army Regulation 5-1 to fully establish the procedures, working relationships, and information base needed to effectively manage Army business processes and systems. Although the Army's EA-informed decisionmaking process impacts many areas of business operations, the best indicator of its success is in the modernization of the Army's business systems. Since its inception, the ABEA-supported portfolio management methodology has been used to sunset over 500 (out of more than 800) IT investments in the Army's Business Mission Area portfolio.

Figures D.1–D.3 show some of the most useful visualizations and analytical products. Singly and in combination, they display the status of activities toward modernizing the IT business system portfolio and enable "what-if" analyses of accelerating the termination of legacy systems, delaying out-year system releases, and changing the fielding timeline for sunset of legacy systems. The end result is objective, supportable decisionmaking affecting system planning, funding, and fielding.

[149] Army Regulation 5-1, *Management of Business Operations*, Department of the Army, U.S. Department of Defense, November 12, 2015.

Figure D.1. Gartner's LEAD Construct

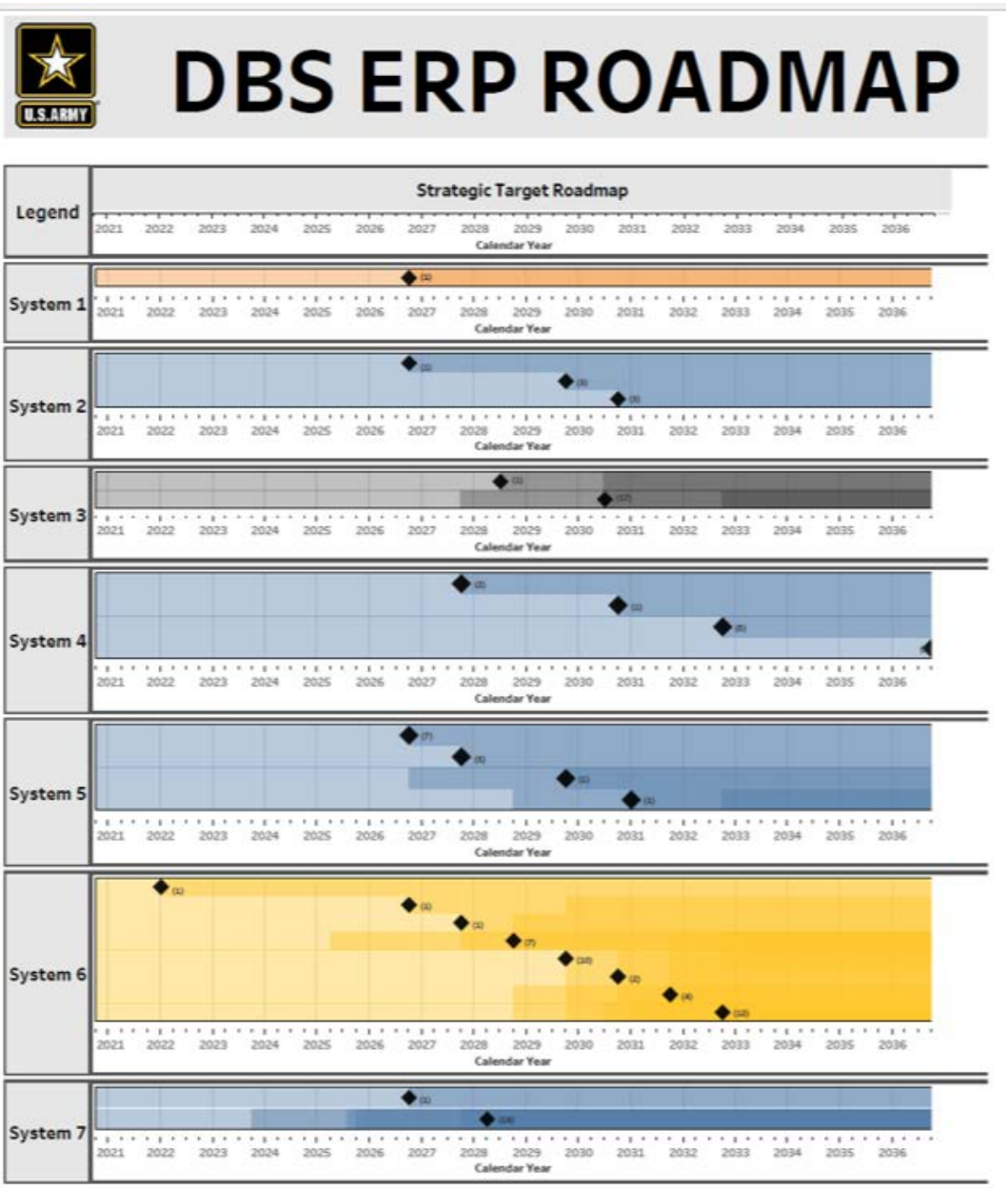


SOURCE: Adapted from Marco Temaner, "EA-Enabled Portfolio Management," briefing slides, PEO Enterprise, Department of the Army, U.S. Department of Defense, undated, Not available to the general public. Redacted for use in this report by Temaner.

Figure D.2. ABEA Application of LEAD Construct for Portfolio Management

SOURCE: Adapted from Temaner, undated. Redacted for use in this report by Temaner.

Figure D.3. Army DBS Enterprise Resource Planning Roadmap



SOURCE: Adapted from Temaner, undated. Redacted for use in this report by Temaner.

The core data underlying these analytics and visualizations is maintained in a distilled set of DODAF products. Beginning with the E2E processes inherited from the DoD level, the Army adds a capability view (CV-2), operational views (OV-3 and OV-5a), a system view (SV-1), and a conceptual data view (DIV-1). Additional DODAF reference models are incorporated as necessary for whatever task or question is at hand, in a dataset kept evergreen and curated by the Army chief enterprise architect. See Figure D.4.

Figure D.4. Army System Sunset Dashboard

SOURCE: Adapted from Temaner, undated. Redacted for use in this report by Temaner.

Appendix E

Background on DoD's Financial Statement Audit

Overview of Financial Statement Audits

Two major types of audits conducted within the U.S. government are performance audits and financial audits.[150] Performance audits examine the efficacy and efficiency of programs. These types of audits are largely outside the scope of financial audits but related to business process reengineering efforts discussed later in this appendix. Financial audits include financial statement audits that "provide financial statement users with an opinion by an auditor on whether an entity's financial statements are presented fairly."[151] The Chief Financial Officer Act of 1990 required annual financial statement audits of all federal departments.[152] Other types of financial audits include audits with narrower scope, such as examining compliance with LRPs.

Financial statement audit results are commonly categorized in four ways:[153]

- **Disclaimer of opinion.** The auditor does not issue an opinion when the auditor is "unable to obtain sufficient appropriate audit evidence on which to base an opinion."[154] In the FY 2024 report, 15 of the 28 reporting entities received a disclaimer, including all military services except the U.S. Marine Corps (USMC).
- **Adverse opinion.** The auditor concludes that that "the financial statements as a whole are inaccurate or do not comply with generally accepted accounting principles." Such an opinion would likely be considered a step down from a disclaimer of opinion, though it might indicate that reporting entity was more auditable in the sense that it could provide necessary evidence to the auditor, and therefore remediation could be easier. No DoD reporting entities received an adverse opinion in FY 2024.
- **Qualified opinion.** The auditor concludes that the financial statement is deemed to contain "a departure from generally acceptable accounting principles—the effect of which is material—but the auditor has concluded not to express an adverse opinion."[155] A qualified opinion is

[150] For a full overview of U.S. government audit methods, see GAO, *Government Auditing Standards: 2024 Revision*, GAO-24-106786, February 2024.

[151] GAO, 2025, p. 9.

[152] For a thorough overview of the history of financial statement audits in DoD, see Appendix B of Warren et al., 2024.

[153] For an overview of financial statement audit results, see p. 1 of Warren et al., 2024.

[154] DoD, 2024c, p. 50.

[155] Warren et al., 2024, p. 1.

sometimes considered a "favorable opinion" because it represents an improvement from a disclaimer. In FY 2024, one of 28 DoD reporting entities received a qualified opinion.

- **Unmodified opinion.** Also called an "unmodified audit opinion" or a "clean opinion." The auditor "finds that the financial statement does not contain any material misstatement, complies with all the applicable reporting standards, and presents a true and fair view."[156] The USMC received unmodified opinions in both FY 2023 and FY 2024, though reporting of this success was delayed until after the DoD Financial Report was released for both years.

DoD's financial statement currently consolidates financial statements from 28 different stand-alone reporting entities. Only nine of these reporting entities received unmodified opinions, while 15 received disclaimers of opinion, one received a qualified opinion, and three had pending opinions. Due to the substantial share of reporting entities with a disclaimer of opinion, which represented "at least 44 percent of the DoD's total assets and at least 68 percent of the DoD's total budgetary resources," DoD received a disclaimer of opinion.[157] DoD is the only federal agency that has never obtained an unmodified opinion; the last agency to achieve its first clean opinion was the Department of Homeland Security in FY 2013, while DoD did not conduct its first audit until FY 2018 and has received disclaimers of opinion in that and all subsequent audits.[158]

Compliance Areas Most Relevant to the DBEA

At the highest level, the most important areas for DoD to ensure compliance are detailed in its Agency Financial Report, which includes financial statements; DoD's Statement of Assurance, which provides DoD management's statements on its compliance with applicable laws; and the Independent Auditor's Report, which provides the auditor's opinion on the financial statements and other issues, such as DoD's compliance with applicable laws.[159]

A primary focus area of the Statement of Assurance within the annual financial report is the "effectiveness of internal controls over financial reporting."[160] This analysis identified 50 material weaknesses—i.e., significant deficiencies that could result in substantial misstatements of the financial statements. The analysis of internal controls focuses on requirements from the following sources:

- **The Federal Managers' Financial Integrity Act (FMFIA) of 1982**, which amended the Accounting and Auditing Act of 1950. It requires reports on finances and requires plans to improve financial management. FMFIA Sec. 2 added requirements to develop accounting and

[156] Warren et al., 2024, p. 1.

[157] DoD, 2024c, p. 73

[158] Asif A. Khan, *DoD Financial Management: Additional Actions Needed to Achieve a Clean Audit Option on DoD's Financial Statements*, U.S. Government Accountability Office, GAO-23-105784, May 15, 2023.

[159] For FY 2024, see DoD, 2024c.

[160] DoD, 2024c, p. 52.

internal controls—processes designed to promote accuracy and compliance in financial reporting—and report on the effectiveness of these controls.[161]

- **U.S. Office of Management and Budget (OMB) Circular No. A 123, "Management's Responsibility for Enterprise Risk Management and Internal Control,"** which developed processes to comply with FMFIA Sec. 2. DoD has implemented these processes through its RMIC program, described later in this section.

For FY 2024, DoD reported 94 material weaknesses across 32 business and operations areas concerning the effectiveness of internal controls over financial reporting, citing noncompliance with FMFIA Sec. 2 and OMB Circular No. A-123 requirements.[162]

Another focus area of the Statement of Assurance is the "compliance of DoD financial information statements" with applicable laws. These laws include the following:

- **Section 4 of the FMFIA** requires that annual financial reports provide detail "on whether the agency's accounting system conforms to the principles, standards, and related requirements prescribed by the Comptroller General."[163]
- **The FFMIA of 1996** "requires the 24 CFO [Chief Financial Officer] Act agencies to implement and maintain financial management systems, that comply substantially with (1) Federal Financial Management Systems Requirements, (2) Federal accounting standards, and (3) the U.S. Government Standard General Ledger (USSGL) at the transaction level."[164]
- **OMB Circular No. A 123, Appendix D, "Management of Financial Management Systems—Risk and Compliance,"** provides guidance on determining compliance with FFMIA. It includes a checklist of items necessary for compliance, summarized in later in this appendix.[165] In addition, the circular says that external service providers "should provide customer agencies with a Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (also known as a SOC 1)."[166] These are a type of attestation provided by auditors governed by the Association of International Certified Professional Accountants Statement of Standards for Attestation Engagements (SSAE) No. 18. The FY 2024 DoD Agency Financial Report says that auditors conducted 27 SSAE examinations on 35 systems owned by eight DoD service providers.[167]
- **Title 10, Section 240g, "Defense Business Audit Remediation Plan,"** requires a plan to make changes to DoD's business system needed for the financial audit. This includes "a

[161] See Public Law 97-255, Federal Managers Financial Integrity Act of 1982; Section 2, September 8, 1992. Codified in U.S. Code, Title 31, Money and Finance, Subtitle III, Financial Management; Chapter 35, Accounting and Collection; Subchapter II, Accounting Requirements, Systems, and Information; Section b.

[162] DoD, 2024c, p. 52.

[163] See Public Law No. 97-255, Federal Managers Financial Integrity Act of 1982; Section 4, September 8, 1992; U.S. Code, Title 31, Money and Finance, Subtitle III, Financial Management; Chapter 35, Accounting and Collection; Subchapter II, Accounting Requirements, Systems, and Information; Section d; Paragraph 2; Clause B.

[164] Shalanda D. Young, "Appendix D, Management of Financial Management Systems—Risk and Compliance," memorandum, U.S. Office of Management and Budget, Executive Office of the President, December 23, 2022, p. 2.

[165] Young, 2022, pp. 18–21.

[166] Young, 2022, p. 4.

[167] DoD, 2024c, p. 50.

current accounting of the defense business systems of the Department of Defense that will be introduced, replaced, updated, modified, or retired."[168]

For FY 2024, DoD was unable to provide assurance that its financial management systems comply with these LRPs and further identified three instances of nonconformance to the requirements.[169]

Also included in the DoD financial statement, the Office of Inspector General's *Report on Compliance with Laws, Regulations, Contracts, and Grant Agreements* reports on compliance issues that arose in the financial statement audit, rather than a full scope of all potential compliance needs. Nevertheless, the report identifies six statutes (including the FFMIA Acts of 1982 and 1996) where DoD is noncompliant or potentially noncompliant.

Clean audit opinions do not necessarily rely on across-the-board compliance in all areas. Many of the statutes for which DoD must be legally compliant have limited applicability to the accuracy of financial reporting. There are also complex trade-offs between financial systems and controls. Although the DoD Financial Report promotes financial system modernization as "critical to efficiently respond to warfighter needs, sustain public confidence in the Department's stewardship of taxpayer funds, and support the path to full auditability," "outdated, non-compliant systems" are not an absolute barrier to audit success because controls can be developed to overcome system limitations, though these controls are potentially manpower intensive and can increase the risk of errors.[170] As an example, in FY 2023, the USMC received an unmodified audit opinion even though the external auditors' tests of FFMIA compliance "disclosed instances in which the USMC's financial management systems did not substantially comply with federal financial management systems requirements, applicable federal accounting standards or the USSGL [U.S. Standard General Ledger]."[171]

How Can DoD Achieve a Successful Financial Statement Audit?

Getting to a clean audit is not necessarily straightforward. DoD has been attempting to get there for decades, beginning in earnest with the FIAR program in 2005.[172] Funding was established for FIAR-related efforts and sharply increased for most services in the aftermath of the first audit in FY 2018 as DoD shifted from audit readiness to remediation.[173] Prior to first audits, FIAR efforts prioritized achieving "audit readiness validation" with target dates for independent certification of readiness across different business areas. However, deadlines were missed, and eventually—as the 2018 audit approached—all services began self-certifying that they were audit ready.

Following the first audit, DoD and the services have taken a similar approach as they and their independent auditors have identified material weaknesses, and the services have developed prioritized

[168] U.S. Code, Title 10, Section 240g, Sec. (a).

[169] DoD, 2024c.

[170] DoD, 2024c, p. 56.

[171] U.S. Marine Corps, *Fiscal Year 2024 Agency Financial Report*, February 2025, p. 54.

[172] FIAR was renamed to Financial Improvement and Audit Remediation following the completion of DoD's first financial statement audit for FY 2018.

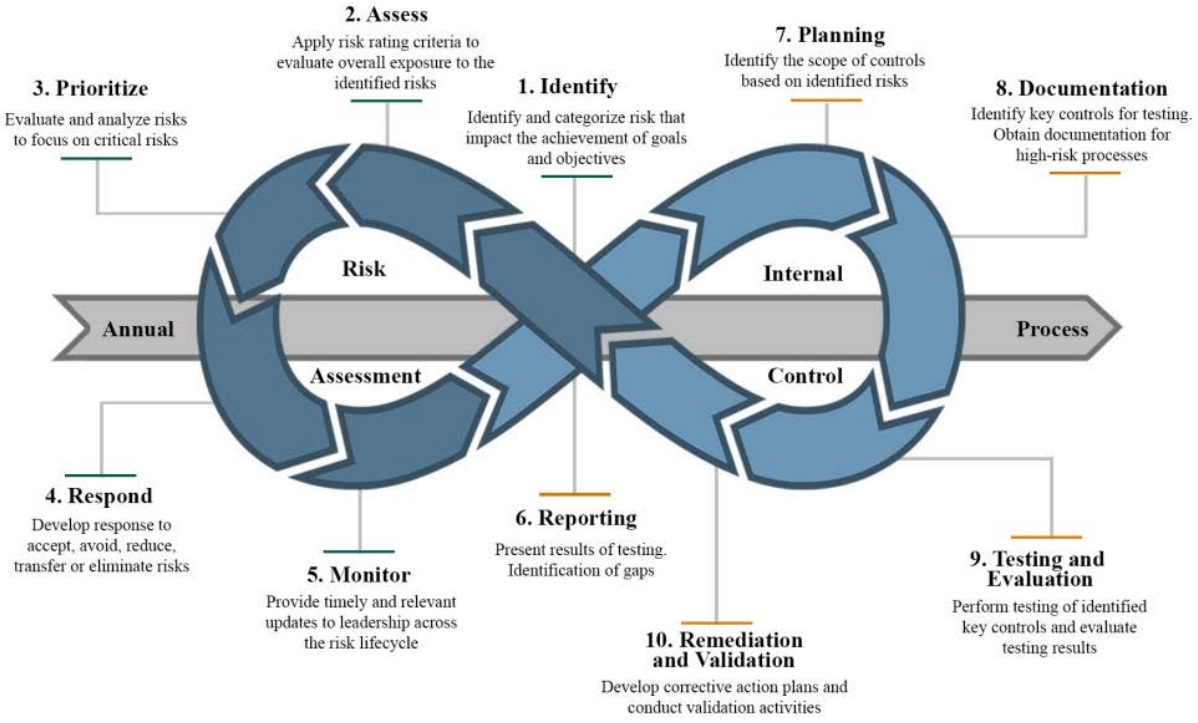
[173] For a comprehensive review of the history of DoD financial statement audit efforts and resourcing, see Appendix B of Warren et al., 2024.

road maps with FY goals to downgrade those material weaknesses. As mentioned in the earlier USMC example, not all material weaknesses need to be remediated to achieve a successful financial statement audit. Road maps typically prioritize material weaknesses that pose the most risk to financial statements. For example, Funds Balance with Treasury is a high priority because it represents the funding authority for DoD components to conduct their activities.

Independent auditors also identify specific weaknesses in NFRs, which components work to address as part of their efforts to address the broader material weaknesses. This approach can seem like running in place, however, because each audit cycle identifies NFRs at nearly the same rate that DoD can remediate them. Between 2019 and 2022, there were about 3,000 NFRs across DoD, and around 25 percent per year have been remediated, though with new NFRs the total number has stayed relatively constant.[174]

Efforts to remediate NFRs and materials weaknesses often focus on addressing specific issues by adding or changing and internal controls, and possibly with some supporting changes to financial systems. DoD Instruction 5010.40 provides a detailed process for identifying and managing risks through internal controls.[175] Figure E.1 shows a representation of this process.[176]

Figure E.1. RMIC Program Process



SOURCE: Reproduced from DoD, 2024c, p. 55.

[174] See Figure B.2 in Warren et al., 2024, for details.

[175] DoD Instruction 5010.40, *DoD Enterprise Risk Management and Risk Management and Internal Control Program*, DoD Directives Division, Executive Services Directorate, Washington Headquarters Services, December 11, 2024.

[176] DoD Instruction 5010.40 has been updated since the figure was created.

As discussed earlier, Appendix D of Circular No. A 123, "Management of Financial Management Systems—Risk and Compliance," provides a checklist for systems to achieve FFMIA compliance. We summarized the checklist as follows:[177]

- 1.0 Manage Financial Information Management and Reporting
  - 1.1 Correct financial records
  - 1.2 Timely and accurate financial information for agency managers
  - 1.3 Timely and accurate financial information for stakeholders like the President, Congress, and the public
  - 1.4 Timely and accurate financial information to help achieve good performance
- 2.0 Financial Management and Internal Controls
  - 2.1 Use internal controls to ensure spending is legal and within amount available.
  - 2.2 Perform effective financial management operations.
  - 2.3 Reduce waste, loss, or misuse of government resources.
  - 2.4 Manage financial management systems security risks.

As the FY 2023 USMC clean audit demonstrates, comprehensive remediation of financial system problems is not necessarily a prerequisite for achieving a clean audit opinion. USMC was able to achieve audit success despite having financial systems that are not FFMIA compliant. This led to three unresolved material weaknesses that the USMC addressed through what was described to us as a "brute-force approach," creating labor intensive controls to ensure that business processes produce reliable financial information.

Law requires that DoD achieve a clean audit by the end of 2028.[178] Given this short timeline, it is likely that audit remediation efforts will focus more on labor intensive controls than comprehensive financial system modernization. It remains to be seen whether this approach, which worked for the USMC, a relatively small service, can work for larger, more complex services.[179] Even if this approach achieves a clean audit by the end of 2028, a clean audit will likely be challenging to sustain without more fundamental, more transformational changes that include fundamental improvements and modernization of financial systems. Such a transformational approach would likely also magnify the benefits for a clean audit by enabling more effective and more efficient business processes.

According to the FY 2024 DoD Financial Report, DoD is engaging in some efforts to achieve these financial system improvements through an Audit Remediation Plan developed in accordance with Title 10, Section 240(g). The discussion focuses on two related lines of effort to transform its systems. First, DoD is rationalizing systems "that were important to financial controls over financial reporting, further simplifying the portfolio of systems."[180] This resulted in the elimination of ten

[177] Young, 2022, pp. 18–21.

[178] DoD, 2024c, p. 6.

[179] See Katharina Ley Best and Drake Warren, "Digging In: The Army's Promising Path to Real Change in Audit," commentary, RAND Corporation, December 13, 2024.

[180] DoD, 2024c, p. 56.

systems in FY 2024. Second, DoD's long term financial system strategy focuses on building and improving the department's ERP systems because they "are integral to implementing the FM [financial management] business process improvements necessary for effective internal controls over financial reporting, achieving the planned target environment, reducing the number of vulnerable systems, and sustaining an auditable systems environment."[181]

[181] DoD, 2024c, p. 57.

Appendix F

Industry Enterprise Architecture Approaches

This appendix provides overviews of selected industry enterprise architecture approaches to supplement the industry frameworks discussed earlier in the report.

Microsoft

Microsoft's enterprise architecture (EA) approach is centered on enabling organizations to achieve agility, scalability, and innovation through integrated solutions and frameworks. At the core of its methodology is the Microsoft Cloud Adoption Framework, which provides structured guidance for organizations to plan, adopt, and optimize cloud technologies in alignment with their business objectives.[182] This framework emphasizes iterative development, operational efficiency, and adaptability, helping enterprises modernize legacy systems and create scalable architectures that support digital transformation. Microsoft's EA approach also leverages its robust suite of tools, including Azure, Power Platform, and Dynamics 365, to provide advanced capabilities for data integration, process automation, and customer relationship management. These tools are designed to encourage collaboration across teams and business units, facilitating federated architectural models that align with diverse organizational needs.[183]

A key differentiator of Microsoft's EA strategy is its focus on leveraging emerging technologies, such as AI, ML, and the internet of things (IoT), to enable intelligent decisionmaking and operational excellence. For example, Azure AI services and Azure Machine Learning empower organizations to analyze large scale data and derive actionable insights, while IoT solutions enable real-time monitoring and optimization of business processes.[184] Microsoft's EA approach also prioritizes security and compliance, offering built-in governance tools and frameworks to help organizations address cybersecurity risks and regulatory requirements.[185] By integrating these technologies and practices, Microsoft positions EA as a strategic enabler of business outcomes, such as revenue growth, enhanced customer experiences, and operational efficiency. Through its comprehensive approach, Microsoft

[182] Microsoft Learn, undated-c.

[183] Microsoft, homepage, undated.

[184] Microsoft Learn, "Azure AI Services Documentation," webpage, undated-a; Microsoft Azure, "Azure IoT," webpage, undated.

[185] Microsoft Learn, homepage, undated-b.

continues to lead the industry in providing scalable, secure, and innovative enterprise architecture solutions tailored to the needs of modern businesses.[186]

Amazon

Amazon Web Services (AWS) has established itself as a leader in EA by providing a highly scalable, flexible, and innovative cloud-based framework that empowers organizations to achieve digital transformation. At the core of AWS's EA approach is the AWS Well-Architected Framework, which provides best practices and guidance for designing cloud architectures that are secure, reliable, performant, cost efficient, and sustainable.[187] This framework helps enterprises build resilient systems tailored to their specific business needs while offering tools to continuously optimize workloads. AWS also emphasizes the importance of automation and agility, enabling organizations to rapidly deploy applications, scale resources on demand, and adapt to changing market conditions. By leveraging AWS's extensive suite of services, such as EC2 for compute, S3 for storage, and Lambda for serverless computing, enterprises can modernize their IT infrastructure and reduce dependency on legacy systems.

A key element of AWS's EA strategy is its focus on enabling data-driven decisionmaking and advanced analytics through such services as Amazon Redshift, AWS Glue, and Amazon QuickSight. These tools allow organizations to integrate and analyze large scale data, providing actionable insights that drive business outcomes. AWS also leads the industry in harnessing emerging technologies, such as AI, ML, and IoT. Services such as Amazon SageMaker facilitate the development and deployment of ML models, while AWS IoT Core enables real-time monitoring and optimization of connected devices.[188] Additionally, AWS prioritizes security and compliance, offering robust governance tools, such as AWS Identity and Access Management and AWS Security Hub, to help organizations mitigate risks and meet regulatory requirements.[189]

AWS frames enterprise architecture as a key component in enabling business transformation. By emphasizing scalability, automation, emerging technologies, and data-driven solutions, the approach could provide organizations with a means to enhance operational efficiency and support growth and innovation. The platform is diverse and can help facilitate collaboration through offering tools that assist in optimization of enterprise architecture designs that support resilience, support adaptability, and are aligned with organizations strategic goals.

Google

Google's EA approach is centered on enabling organizations to innovate, scale, and optimize operations through its cloud-based solutions and advanced technologies. At the forefront of Google's

[186] Microsoft, homepage, undated.

[187] Amazon AWS, undated-d.

[188] Amazon AWS, "Amazon SageMaker," webpage, undated-a; Amazon AWS, "AWS IoT Core Documentation," webpage, undated-c.

[189] Amazon AWS, "AWS Cloud Security," webpage, undated-b.

strategy is Google Cloud's architecture framework, which provides best practices for building secure, scalable, and high-performance systems tailored to business needs.[190] This framework emphasizes automation, agility, and sustainability, helping enterprises modernize legacy systems and embrace digital transformation. Google Cloud offers a robust suite of services, including Compute Engine, Kubernetes Engine, and BigQuery, which enable organizations to deploy applications, manage containerized workloads, and analyze massive datasets. By integrating these tools, Google empowers businesses to create architectures that are adaptable to dynamic market conditions while driving operational efficiency and innovation. A defining feature of Google's EA approach is its focus on leveraging AI and ML to enable intelligent decisionmaking and enhance customer experiences. Tools like Vertex AI and TensorFlow facilitate the development and deployment of ML models, while Google Cloud AI services provide pretrained models for natural language processing, image recognition, and other advanced capabilities.[191] Additionally, Google prioritizes security and compliance through solutions like BeyondCorp Enterprise and Chronicle, which offer zero trust security frameworks and advanced threat intelligence.[192] By combining cutting-edge technologies, data-driven insights, and secure architectures, Google positions itself as a leader in enterprise architecture, enabling organizations to achieve sustainable growth, operational excellence, and innovation in competitive industries.

SAP

SAP's EA approach is designed to help organizations achieve digital transformation and operational excellence by integrating business processes, data, and technology into cohesive systems. At the core of SAP's strategy is the SAP Business Technology Platform, which provides a unified framework for building, managing, and optimizing enterprise applications.[193] This platform combines capabilities such as SAP HANA (High-performance ANalytic Appliance) for real-time data analytics, SAP Integration Suite for seamless system connectivity, and SAP Analytics Cloud for advanced business intelligence. SAP's EA approach emphasizes modularity and scalability, enabling organizations to adapt quickly to changing business needs while reducing complexity. Additionally, SAP leverages emerging technologies like AI, ML, and IoT to enhance decisionmaking and automate processes. By offering tools for governance, compliance, and process optimization, SAP seeks to position EA as a strategic enabler for driving innovation, improving customer experiences, and achieving measurable business outcomes in competitive industries.[194]

[190] Google Cloud, homepage, undated-a.

[191] Google Cloud, "Vertex AI Platform: Innovate Faster with Enterprise-Ready AI, Enhanced by Gemini Models," webpage, undated-c.

[192] Google Cloud, "Protect Your Organization with Google Cloud Security Solutions," webpage, undated-b.

[193] SAP, homepage, undated.

[194] SAP, undated.

Abbreviations

ABEA	Army business enterprise architecture
ADM	Architecture Development Method
AGA	Australian Government Architecture
AI	artificial intelligence
API	application programming interface
AUSDAF2	Australian Defence Architecture Framework 2
AWS	Amazon Web Services
BA	business architecture
BEA	business enterprise architecture
BTA	Business Transformation Agency
CAF	Canadian Armed Forces
CANFORGEN	Canadian Forces General Message
CCA	Clinger Cohen Act
CDAO	Chief Digital and Artificial Intelligence Office
CFB	Cross Functional Board
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMO	Chief Management Officer
COTS	commercial off-the-shelf
CV	capability view
DAF	Defence Architecture Framework
DBC	Defense Business Council
DBEA	defense business enterprise architecture
DBRA	Defence Business Reference Architecture
DBS	defense business system
DCMO	Deputy Chief Management Officer
DITPR	Defense Information Technology Portfolio Repository
DND	Department of National Defence
DNDAF	Department of National Defence Architecture Framework
DoD	U.S. Department of Defense
DODAF	Department of Defense Architecture Framework
E2E	end-to-end
EA	enterprise architecture
EAP	Enterprise Architecture Programme

ERP	enterprise resource planning
FEAF	Federal Enterprise Architecture Framework
FFMIA	Federal Financial Management Improvement Act
FIAR	Financial Improvement and Audit Readiness
FMFIA	Federal Managers' Financial Integrity Act
FMMP	Financial Management Modernization Program
FVEY	Five Eyes
FY	fiscal year
GAO	U.S. Government Accountability Office
GEA-NZ	Government Enterprise Architecture for New Zealand
ICT	information and communications technologies
IDA	Integrated Defence Architecture
IoT	internet of things
IT	information technology
JCIDS	Joint Capabilities Integration and Development System
LRPs	laws, regulations, and policies
ML	machine learning
MoD	Ministry of Defence
MODAF	Ministry of Defence Architecture Framework
NAF	NATO Architecture Framework
NAFv4	NATO Architecture Framework, version 4
NATO	North Atlantic Treaty Organization
NDAA	National Defense Authorization Act
NFR	Notices of Findings and Recommendations
OA	operational activity
OMB	U.S. Office of Management and Budget
OSD	Office of the Secretary of Defense
OV	operational view
PPBE	Planning, Programming, Budgeting, and Execution
RMIC	Risk Management and Internal Control
SME	subject matter expert
SSAE	Statement of Standards for Attestation Engagement
SV	system view
TOGAF	The Open Group Architecture Framework
UAF	Unified Architecture Framework
UK	United Kingdom
UKRA	UK Reference Architecture
USMC	U.S. Marine Corps
USSGL	U.S. Standard General Ledger
WG	working group

References

Ahlemann, Frederik, Eric Stettiner, Marcus Messerschmidt, and Christine Legner, eds., *Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments*, Springer, 2012.

Amazon AWS, "Amazon SageMaker," webpage, undated-a. As of August 15, 2025: https://aws.amazon.com/sagemaker/

Amazon AWS, "AWS Cloud Security," webpage, undated-b. As of August 15, 2025: https://aws.amazon.com/security/

Amazon AWS, "AWS IoT Core Documentation," webpage, undated-c. As of August 15, 2025: https://docs.aws.amazon.com/iot/

Amazon AWS, "AWS Well-Architected," webpage, undated-d. As of August 15, 2025: https://aws.amazon.com/architecture/well-architected/

Architecture Capability Team, *NATO Architecture Framework*, Consultation, Command & Control Board, North Atlantic Treaty Organization, September 2020.

Army Regulation 5-1, *Management of Business Operations*, Department of the Army, U.S. Department of Defense, November 12, 2015.

Australian Government, "Australian Government Architecture," webpage, undated. As of August 15, 2025: https://architecture.digital.gov.au/

Best, Katharina Ley, and Drake Warren, "Digging In: The Army's Promising Path to Real Change in Audit," commentary, RAND Corporation, December 13, 2024. https://www.rand.org/pubs/commentary/2024/12/digging-in-the-armys-promising-path-to-real-change.html

Burns, Peter, Michael Neutens, Daniel Newman, and Tim Power, *Building Value Through Enterprise Architecture: A Global Study*, Booz & Company, 2009.

CDAO—*See* Chief Digital and Artificial Intelligence Office.

Chief Digital and Artificial Intelligence Office, "Analytic Tools," webpage, undated. As of July 24, 2025: https://www.ai.mil/Initiatives/Analytic-Tools/

Commission on Planning, Programming, Budgeting, and Execution Reform, *Defense Resourcing for the Future: Final Report*, March 2024.

Defense Acquisition University, "Adaptive Acquisition Framework Document Identification: Software Acquisition Pathway (SWP)," webpage, undated. As of August 15, 2025: https://www.dau.edu/aafdid/swa

Defense Business Board, *The Chief Management Office of the Department of Defense: An Assessment*, DBB FY 20-01, June 1, 2020.

Department of Defence, "Defence Business Reference Architecture," briefing slides, Australian Government, 2015.

Department of Finance and Deregulation, *Australian Government Architecture Reference Models*, Australian Government, August 2011.

Department of National Defence, *Promulgation of the Department of National Defence and Canadian Forces Architecture Framework (DNDAF) and the Defence Architecture Data Model (DADM)*, Government of Canada, January 2008.

DoD—*See* U.S. Department of Defense.

DoD Instruction 5010.40, *DoD Enterprise Risk Management and Risk Management and Internal Control Program*, DoD Directives Division, Executive Services Directorate, Washington Headquarters Services, December 11, 2024.

DoD IT Portfolio Repository, "Defense Business Systems Data Report," spreadsheet, December 2024.

Farahbod, R., A. Guitouni, and E. Bossé, *Towards a Comprehensive DND/CF Enterprise Architecture Methodology: A Critical Review DNDAF for an Integrated C2 Capability Development*, Defence Research and Development Canada, June 2013.

Gartner, "Build Your Enterprise Architecture Discipline," webpage, undated. As of August 15, 2025: https://www.gartner.com/en/information-technology/topics/enterprise-architecture

GAO—*See* U.S. Government Accountability Office.

Gerber, Aurona, Pierre le Roux, Carike Kearney, and Alta van der Merwe, "The Zachman Framework for Enterprise Architecture: An Explanatory IS Theory," *Responsible Design, Implementation and Use of Information Communication Technology*, I3E 2020, *Lecture Notes in Computer Science*, Vol. 12066, April 1, 2020.

Gershon, Peter, *Review of the Australian Government's Use of Information and Communication Technology*, Australian Government Information Management Office, August 2008.

Gerth, Anthony B., and Joe Peppard, "The Dynamics of CIO Derailment: How CIOs Come Undone and How to Avoid It," *Business Horizons*, Vol. 59, No. 1, January–February 2016.

Gibel, T. B., "Steadying the Course: Enterprise Architecture in the RCN," Canadian Forces College, Canadian Armed Forces, 2015.

Google Cloud, homepage, undated-a. As of August 15, 2025: https://cloud.google.com/

Google Cloud, "Protect Your Organization with Google Cloud Security Solutions," webpage, undated-b. As of August 15, 2025: https://cloud.google.com/solutions/security

Google Cloud, "Vertex AI Platform: Innovate Faster with Enterprise-Ready AI, Enhanced by Gemini Models," webpage, undated-c. As of August 15, 2025: https://cloud.google.com/vertex-ai

Google Cloud, "Google Cloud Well-Architected Framework," webpage, last reviewed October 11, 2024. As of August 15, 2025: https://cloud.google.com/architecture/framework

Government of the United Kingdom, "Guidance: MOD Architecture Framework," webpage, last updated August 7, 2020. As of August 15, 2025: https://www.gov.uk/guidance/mod-architecture-framework

Hanks, Christopher, "A Critical Examination of the DoD's Business Management Modernization Program," *Proceedings of the Second Annual Acquisition Research Symposium*, Naval Postgraduate School, May 1, 2005.

Hanson, Jack, "The Strategic Architecture Behind Our Digital Future," *DWP Digital* blog, August 11, 2022.

Harishankar, Ray, and S. Kevin Daley, "Actionable Business Architecture," paper presented at 2011 IEEE Conference on Commerce and Enterprise Computing, 2011.

Hause, Matthew, Graham Bleakley, and Aurelijus Morkevicius, "Technology Update on the Unified Architecture Framework (UAF)," *INCOSE International Symposium*, Vol. 26, No. 1, July 2016.

HM Revenue and Customs, *UK Government Reference Architecture: Government ICT Strategy*, January 2012.

Hue, Meredith, "An Analysis of SE and MBSE Concepts to Support Defence Capability Acquisition," Department of Defence, Australian Government, September 2014a.

Hue, Meredith, "A Review of Enterprise Architecture Use in Defence," Department of Defence, Australian Government, September 2014b.

Iyamu, Tiko, and Irja Shaanika, "The Factors of Enterprise Business Architecture Readiness in Organisations," *Enterprise Information Systems*, 2022.

Kang, Dongwoo, Jeongsoo Lee, and Kwangsoo Kim, "Alignment of Business Enterprise Architecture Using Fact-Based Ontologies," *Expert Systems with Applications*, Vol. 37, No. 4, April 2010.

Khan, Asif A., *DoD Financial Management: Additional Actions Needed to Achieve a Clean Audit Option on DoD's Financial Statements*, U.S. Government Accountability Office, GAO-23-105784, May 15, 2023.

Lankhorst, Marc, *Enterprise Architecture at Work: Modeling, Communication and Analysis*, Springer, 2017.

Lankhorst, Marc M., Henderick Alex Proper, and Henk Jonkers, "The Architecture of the ArchiMate Language," paper presented at 14th International Conference on Exploring Modeling Methods in Systems Analysis and Design, 2009.

Levine, Peter, *Defense Management Reform: How to Make the Pentagon Work Better and Cost Less*, Stanford University Press, 2020.

Lukashina, Elena V., Alexandr V. Lukashin, and Valery I. Bezrukov, "The Use of Artificial Intelligence Technologies in Building Business Architectures Within the Framework of the 'Green Economy,'" *International Scientific Conference Energy Management of Municipal Facilities and Environmental Technologies*, Vol. 458, 2023.

Mehta, Aaron, and Ashley Roque, "Pentagon Seeks to Shift $50B in Planned Funding to New Priorities in FY26," *Breaking Defense*, February 19, 2025.

Microsoft Azure, "Azure IoT," webpage, undated. As of August 15, 2025: https://azure.microsoft.com/en-us/solutions/iot

Microsoft, homepage, undated. As of August 15, 2025: https://www.microsoft.com/

Microsoft Learn, "Azure AI Services Documentation," webpage, undated-a. As of August 15, 2025: https://docs.azure.cn/en-us/ai-services/

Microsoft Learn, homepage, undated-b. As of August 15, 2025:
https://learn.microsoft.com/

Microsoft Learn, "Microsoft Cloud Adoption Framework for Azure," webpage, undated-c. As of August 15, 2025:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/

Nather, Sarah, "BEA Development and Implementation Way Forward," briefing slides, U.S. Department of Defense Chief Information Officer, March 2024.

New Zealand Government, "Enterprise Architecture," webpage, undated. As of August 15, 2025:
https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/government-enterprise-architecture

New Zealand Government, *Government Enterprise Architecture*, June 2015.

New Zealand Government, "Overview of the GEA-NZ Framework," webpage, last updated March 1, 2021. As of August 15, 2025:
https://dns.govt.nz/standards-and-guidance/technology-and-architecture/government-enterprise-architecture/gea-nz-framework/dimensions-of-the-gea-nz-framework/overview-of-the-gea-nz-framework

New Zealand Government, "Redevelopment of the GEA-NZ Framework," webpage, last updated November 21, 2024. As of August 15, 2025:
https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/government-enterprise-architecture/gea-nz-framework/redevelopment

New Zealand Government, "About the GEA-NZ Framework," webpage, last updated February 10, 2025. As of August 15, 2025:
https://dns.govt.nz/standards-and-guidance/technology-and-architecture/government-enterprise-architecture/gea-nz-framework/about-the-gea-nz-framework

Office of the Under Secretary of Defense (Comptroller), *Defense Financial Improvement and Audit Readiness Plan*, U.S. Department of Defense, December 2005.

Office of the Under Secretary of Defense (Comptroller), *Financial Improvement and Audit Readiness Plan: FIAR Plan*, U.S. Department of Defense, March 2008.

Office of the Under Secretary of Defense (Comptroller), *Financial Improvement and Audit Readiness (FIAR) Plan Status Report*, U.S. Department of Defense, November 2017.

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, *Financial Improvement and Audit Readiness (FIAR) Guidance*, U.S. Department of Defense, April 2017.

Pechacek, Julie, Alan Gelder, Amrit Romana, Ethan Novak, Kathy Conley, Cheryl Green, Dina Eliezer, P. M. Picucci, George Kennedy, and Cullen Roberts, *Considerations for Implementing a Defense Personnel Research Environment*, Institute for Defense Analyses, September 2018.

Public Law 97-255, Federal Managers Financial Integrity Act of 1982; Section 2, September 8, 1992. Codified in U.S. Code, Title 31, Money and Finance, Subtitle III, Financial Management; Chapter 35, Accounting and Collection; Subchapter II, Accounting Requirements, Systems, and Information; Section b.

Public Law 97-255, Federal Managers Financial Integrity Act of 1982; Section 4, September 8, 1992. U.S. Code, Title 31, Money and Finance, Subtitle III, Financial Management; Chapter 35, Accounting and Collection; Subchapter II, Accounting Requirements, Systems, and Information; Section d; Paragraph 2; Clause B.

Public Law 104-106, National Defense Authorization Act for Fiscal Year 1996; Division E, Information Technology Management Reform, February 10, 1996.

Public Law 105-85, National Defense Authorization Act for Fiscal Year 1998, Division A, Department of Defense Authorizations; Title X, General Provisions; Section 1008, Biennial Financial Management Improvement Plan; Subsection a, Paragraph 1, November 18, 1997.

Public Law 107-107, National Defense Authorization Act for Fiscal Year 2002, Division A, Department of Defense Authorizations; Title X, General Provisions; Subtitle A, Financial Matters; Section 1009, Financial Management Modernization Executive Committee and Financial Feeder Systems Compliance Process; Subsection c, Paragraphs 1 and 2, December 28, 2001.

Public Law 107-314, Bob Stump National Defense Authorization Act for Fiscal Year 2003, December 2, 2022.

Public Law 108-375, Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005, October 29, 2004.

Public Law 115-232, John S. McCain National Defense Authorization Act for Fiscal Year 2019, August 13, 2018.

Public Law 117-263, James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, December 23, 2022.

Public Law 118-31, National Defense Authorization Act for Fiscal Year 2024; Section 922, Independent Assessment of the Defense Business Enterprise Architecture, December 22, 2023.

Ross, Jeanne W., Peter Weill, and David C. Robertson, *Enterprise Architecture as Strategy: Creating a Foundation for Business Execution*, Harvard Business School Press, 2006.

Rumsfeld, Donald, "Financial Management Information Within the Department of Defense," memorandum, U.S. Department of Defense, July 19, 2001.

Sabet, Amr, "BEA History," briefing slides, Infinit-EA, undated.

Saint-Louis, Patrick, Marcklyvens C. Morency, and James Lapalme, "Defining Enterprise Architecture: A Systematic Literature Review," paper presented at 2017 IEEE 21st International Enterprise Distributed Object Computing Conference Workshop, 2017.

SAP, homepage, undated.

SAP Learning, "Enterprise Architect," webpage, undated. As of August 15, 2025: https://learning.sap.com/enterprise-architect

Stewart, J. K., "A Case for Enterprise Architecture in Department of National Defence Strategic Management," Canadian Forces College, Canadian Armed Forces, 2016.

Temaner, Marco, "EA-Enabled Portfolio Management," briefing slides, PEO Enterprise, Department of the Army, U.S. Department of Defense, undated, Not available to the general public.

The TOGAF Standard, Version 9.1, Van Haren Publishing, 2011.

The TOGAF Standard, Version 9.2, The Open Group, 2021.

The TOGAF Standard, Version 9.3, Van Haren Publishing, 2023.

Title 10, Section 2222—*See* U.S. Code, Title 10, Section 2222.

UK Government Digital Service and Central Digital and Data Office, "Develop Your Data and APIs Using a Reference Architecture," webpage, March 22, 2021. As of July 22, 2025: https://www.gov.uk/guidance/develop-your-data-and-apis-using-a-reference-architecture#build-an-architecture-that-promotes-data-exchange-across-government

U.S. Code, Title 10, Armed Forces; Subtitle A, General Military Law; Part I, Organization and General Military Powers; Chapter 9A, Audit; Section 240g, Defense Business Audit Remediation Plan; Section (a).

U.S. Code, Title 10, Armed Forces; Subtitle A, General Military Law; Part IV, Service, Supply, and Property; Chapter 131, Planning and Coordination; Section 2222, Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management.

U.S. Code, Title 40, Public Buildings, Property, and Works; Subtitle III, Information Technology Management; Chapter 113, Responsibility for Acquisitions of Information Technology; Subchapter II, Executive Agencies; Section 11315, Agency Chief Information Officer; Subsection B; Paragraph 2.

U.S. Code, Title 44, Public Printing and Documents; Chapter 36, Management and Promotion of Electronic Government Services; Section 3601, Definitions.

U.S. Department of Defense, *Fulcrum: The Department of Defense Information Technology Advancement Strategy*, undated. As of July 24, 2025: https://dodcio.defense.gov/Portals/0/Documents/Library/FulcrumAdvStrat.pdf

U.S. Department of Defense, *Defense Business Council Charter*, 2012.

U.S. Department of Defense, *2022 National Defense Strategy of the United States of America*, 2022.

U.S. Department of Defense, *Federated DoD Business Enterprise Architecture (BEA) Framework—Modernization of the DoD BEA*, January 2024a.

U.S. Department of Defense, *Department of Defense Business Enterprise Architecture Guidebook*, 2024b.

U.S. Department of Defense, *Agency Financial Report: Fiscal Year 2024*, 2024c.

U.S. Government Accountability Office, *Business Systems Modernization: Strategy for Evolving DOD's Business Enterprise Architecture Offers a Conceptual Approach, but Execution Details Are Needed*, GAO-07-451, April 2007.

U.S. Government Accountability Office, *High-Risk Series: An Update*, GAO-11-278, February 2011.

U.S. Government Accountability Office, *DOD Business Systems Modernization: Governance Mechanisms for Implementing Management Controls Need to Be Improved*, GAO-12-685, June 2012.

U.S. Government Accountability Office, *DOD Business Systems Modernization: Additional Action Needed to Achieve Intended Outcomes*, GAO-15-627, July 2015.

U.S. Government Accountability Office, *Financial Management: DOD Needs to Improve System Oversight*, GAO-23-104539, March 2023a.

U.S. Government Accountability Office, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203, April 2023b.

U.S. Government Accountability Office, *Government Auditing Standards: 2024 Revision*, GAO-24-106786, February 2024.

U.S. Government Accountability Office, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743, February 2025.

U.S. Marine Corps, *Fiscal Year 2024 Agency Financial Report*, February 2025.

U.S. Office of Management and Budget, *Federal Enterprise Architecture Framework (FEAF)*, 2012.

Warren, Drake, Maria McCollester, Katharina Ley Best, Frank Camm, Ryan Consaul, Sandra Kay Evans, Paul W. Mayberry, Lewis Schneider, Nathaniel Edenfield, and Sheervon Husband-Clarke, *Organizing for Army Financial Audit Success: Steering Army Organizations Toward Financial Audit Success*, RAND Corporation, RR-A2409-1, 2024. As of July 2, 2025: https://www.rand.org/pubs/research_reports/RRA2409-1.html

Westerman, George, Didier Bonnet, and Andrew McAfee, *Leading Digital: Turning Technology into Business Transformation*, Harvard Business Review Press, 2014.

Young, Shalanda D., "Appendix D, Management of Financial Management Systems—Risk and Compliance," memorandum, U.S. Office of Management and Budget, Executive Office of the President, December 23, 2022.

NATIONAL DEFENSE RESEARCH INSTITUTE

In this congressionally mandated report, the authors assess the effectiveness of the defense business enterprise architecture (DBEA) as a framework for planning, managing, and integrating defense business systems and its adequacy in informing business process reengineering. They also compare the DBEA with similar models from other U.S. government agencies, foreign governments, and major commercial entities to identify lessons that could be applied to the DBEA. The authors reviewed statutory requirements, U.S. Department of Defense (DoD) and service implementation guidance, and historical documents and guidebooks. They also interviewed stakeholders and conducted coding analysis of the interviews to identify key issues. The authors identified the enterprise architectures and logic frameworks most relevant to the DBEA from international partners and allies. Private-sector analysis focused on identifying industry enterprise architectures and frameworks most relevant to the DBEA's mission for a baseline understanding of components and lessons learned that could be applicable to DoD.

$39.00

ISBN-10 1-9774-1562-8
ISBN-13 978-1-9774-1562-2

www.rand.org

RR-A3535-1