



INSTITUTE FOR DEFENSE ANALYSES

Managing Information System Technology Changes across an Enterprise

William R. Simpson, *Project Leader*

Kevin E. Foltz

December 2018

Approved for public
release; distribution is
unlimited.

IDA Non-Standard
NS D-10378

INSTITUTE FOR DEFENSE
ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882



The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task BC-5-2283, "Architecture, Design of Services for Air Force Wide Distributed Systems," for USAF HQ USAF SAF/CIO A6. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

For more information:

William R. Simpson, Project Leader
rsimpson@ida.org, 703-845-6637

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

© 2018 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

Managing Information System Technology Changes across an Enterprise

Kevin E. Foltz and William R. Simpson
Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, VA 22311
{kfoltz, rsimpson}@ida.org

Abstract:

The goal of information management systems in an enterprise is to make the right information available to the right entities at the right times and in the right formats. The standard approach is to purchase a new system to meet current needs. Patches, work-arounds, and added components satisfy the changing future needs while creating an increasingly complex system, and operational capability slowly degrades over time as complexity builds. The system is then rebuilt from the ground up, at great cost and inconvenience, and the cycle repeats. This paper describes an approach for constant change. Instead of building the best system possible based on today's needs, only to replace it in the future, the goal is a system that is capable of evolving toward a better future in a consistent and directed way. This prevents one-off fixes from lingering, and it keeps the distributed decision-making process aligned toward a common enterprise goal. Components not consistent with future goals are identified and scheduled for replacement. Current practices chosen for expedience are assigned expiration dates to prevent them from becoming solidified in the future architecture. The replacement cycle is applied to components of the system instead of the entire system. This stops the cycle of complete replacements by allowing constant change, which reduces overall cost and maintains a more consistent operational capability.

Introduction

Information systems are complex. They are built using products with configurations, settings, and best practices that can be difficult to understand and implement. The products use protocols, which are instantiated in implementations that themselves have engineering trade-offs and configurations. These implementations build on underlying networking infrastructure, protocols, and configurations, and these rely on algorithms,

mathematics, and physics to work. Just the simple act of loading a web page has built into it a vast array of technologies, configurations, settings, and other considerations developed over many years by thousands of individuals, companies, and other entities and refined by billions of users and trillions of interactions. This situation is only becoming more complex as new protocols, mathematics and physics research, products, and operational guidance are developed.

The first challenge for an enterprise is not just how to build an information-sharing system, but how to even define the goals in such a changing landscape. The goals must be set at the appropriate level. Too high, and they fail to guide real-world choices. Too low, and they become too rigid when new technologies emerge. With the right goals, the second challenge is to understand the past, present, and future. The past is all the systems already purchased and operating. The present is the set of systems being put into place now. The future is the vision for upcoming systems, and the direction in which to move current systems. With this understanding of past, present, and future, the final challenge is to integrate and manage these in a cohesive way. As time progresses, the future becomes the present, the present becomes the past, and the past is retired. This cycle should be continuous in order to preserve a functioning system rather than thrash between new and shiny systems with great promise that quickly become frustrating old systems that no longer function.

Current Approaches

Some current approaches to information system management include the following:

- The Expert
- The Bureaucracy

- The Vendor

The Expert

With the expert approach, a single expert or small group owns the problem and the solution to all information system issues. They plan, coordinate, and direct computer-related activities in an organization; help determine the information technology goals of an organization; and are responsible for implementing computer systems to meet those goals. [1] Their competence enables the enterprise to rely on them for all its needs, and the expert is rarely questioned. This is partly because their competence allows them to make good choices, keep systems running, and respond quickly to requests, but also because no one else in the enterprise is qualified to ask the right questions to challenge them. This approach has the benefits of efficiency, consistency, and good alignment with enterprise goals. However, if the expert is a single person or a small group, this person may have their own hidden agenda or biases that drive their decisions. This would be difficult to stop or even discover. Also, an individual or small group may retire, take another job, or otherwise leave the enterprise scrambling for a replacement. Because the system was maintained by a single person, it may have idiosyncrasies that this person created and kept up with, but others coming into the job would not understand. Thus, changing experts requires a complete system overhaul, where a lot of the accumulated knowledge about the system, its users, and best practices is lost. Relying on these experts can be beneficial in the short term, but they may limit the growth and continuous improvement of the organization. [2]

The Bureaucracy

A bureaucracy can address some of the failings of the expert. It is a system for controlling or managing an organization that is operated by a large number of officials employed to follow rules carefully. [3] Instead of a single person who is largely unaccountable, a bureaucracy documents all of its procedures, processes, and decisions in detail. It often has oversight and periodic reviews as well. This allows the function of the bureaucracy to continue even as the people within it are constantly changing. However, bureaucracies often take a life of their own that can diverge from their original intent due to the tendency of the bureaucracy to try to survive through funding variances and changing

political pressures. Also, bureaucracies are inefficient and slow to change, and they often make decisions based on who complains loudest or who has the most influence instead of who has the best ideas. They lack the accountability of a single person. [4] Where the expert can exercise good judgement on a case-by-case basis, bureaucracies are constrained by their own operating procedures, which do not always fit well with future problems that arise.

The Vendor

Vendors ultimately provide the products that are used to build information-sharing systems. They are current with technology, products, and best-practices. They anticipate future needs and work to meet them in their products. As a result, vendors often have better knowledge than a bureaucracy about how to build a system. Also, many vendors work as integrators to provide cohesive solutions for a related set of information-sharing problems. It is often tempting to go to vendors looking for solutions. However, the vendor goal is profit. Profit can be aligned with providing a good solution, but often in the long term it is not. In particular, vendors often strive to lock customers into their solutions by providing functionality that works well as part of their overall solution but does not integrate with other solutions. [5] When an organization is locked in, the vendor can increase prices until they are close to the significant cost to switch vendors. Comparing vendors or choosing a different vendor is not the solution, because the problem is inherent in the vendors' goals and the structure of the relationship.

The Vision

A new approach is needed to address current problems. Our vision includes the following components:

- Describe design principles and goals
- Document the past, present, and future
- Trickle down from future to present to past
- Dedicate teams to continuously review and update documentation

The first part, where design principles and goals are described, forms the foundation for all later work. Current work on Enterprise Level Security

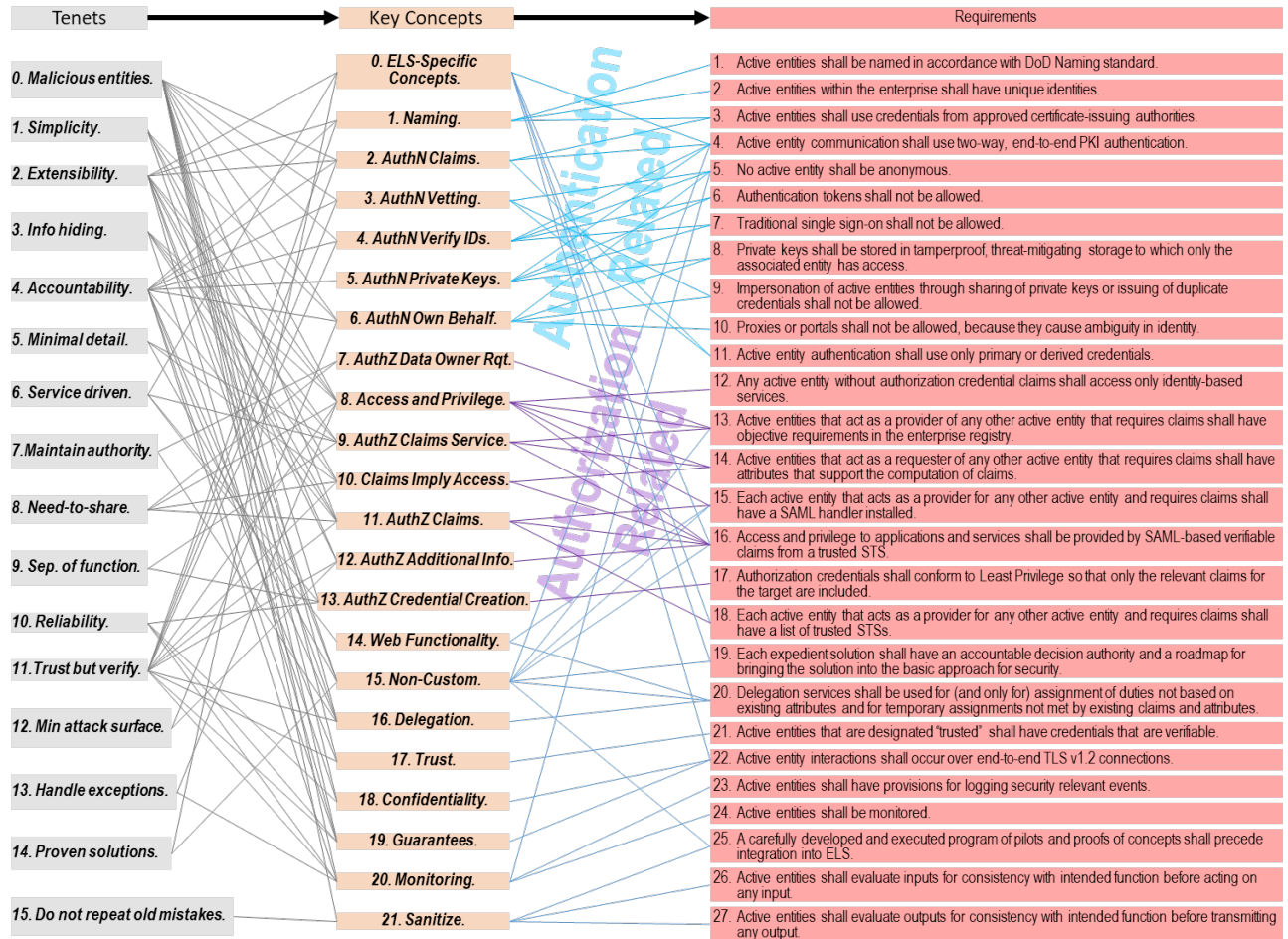


Figure 1. Mapping of Tenets to Concepts to Requirements

(ELS) starts with a set of tenets, as shown in Figure 1. These are basic design principles that are used to build the ELS architecture. Examples include simplicity, assuming malicious entities cannot be kept out of our system, extensibility, and accountability. These basic ideas and goals shape all detailed decisions for the system. Tied to these tenets are a set of key concepts for our system. These include important protocol decisions, the need to name all entities, and the need to authenticate all entities. Unlike the tenets, which could be applied to many different types of systems, the key concepts are related specifically to our information system. Tied to these concepts are a list of requirements. These include specific naming requirements, the requirement for unique identities, and the restriction against anonymity in communications. The requirements are still not particular to any product or service, but they apply generally across many products. These are high-level requirements for the entire information-

sharing system. This basic security model is described in more detail in [6].

Beyond these tenets, principles, and goals are a set of documents that discuss specific technologies. These document the past, present, and future. The future is closely tied to the design principles and goals. This is the "Target Baseline," which consists of documents that describe the goal for the near future for different technologies. The first set of these documents consists of "Scenarios," which describe different mission needs and the questions they raise about how to use technology. The second part consists of "Technical Profiles," which describe how to use different technologies. These include authentication, access control, and other basic security functions. They also include mobile device management, databases, and operating systems, which rely on the basic security documentation and requirements. Scenarios are written as mission needs are identified. Technology

profiles are written as the scenarios raise technology questions.

The scenarios and technology profiles describe the goal for the ideal future state. This is not constrained by current products or best practices. It seeks to apply the design principles and goals to particular technology problems by proposing technical solutions that are consistent with the design goals.

The present-looking documents are the “Implementation Baseline,” which describe current products. Each document provides an assessment of how a currently available product compares against relevant Technical Profile requirements. “Capability Profile” documents bridge the gap between the Target Baseline and Implementation Baseline. These describe the capability a product implements and the relevant target baseline document requirements that apply.

A product with an Implementation Baseline document is not an approved product. It is simply a product that has been analyzed with respect to the goals for the security model and information sharing. With this analysis, it is possible to make informed decisions for risk management. The document identifies shortcomings in security and capability. It quantifies the security risks and provides forms of mitigation that may reduce risk.

The Implementation Baseline documents also include information about product vendor plans for the future, such as whether or when they plan to release an updated version that meets certain requirements or mitigates risks. For example, when setting up an encrypted communication path, a product may use several standard approaches. For many reasons, including vulnerabilities and compromises, the more current standards may be required as part of the baseline. The current release of a product may have implemented Transport Layer Security (TLS) version 1.0. This may not meet the baseline requirement of TLS 1.2 or subsequent. However, the developer may plan to provide TLS 1.2 in its next release. This future-looking assessment can be used to decide whether a product is more or less likely to meet future enterprise needs by comparing their plans to the future goals as stated in the Target Baseline. In some

cases, the product will not be recommended if it is not on a path to satisfy the baseline.

The final set of documents is the “Operational Baseline,” which looks to the past and describes the currently fielded products and their operational rules, configurations, and best practices. Like the implementation baseline, this operational baseline identifies shortcomings in security and capability. It quantifies the security risks and provides forms of mitigation that may reduce that risk. It can also provide an upgrade approach through the implementation baseline for current software that will bring it more in line with the target baselines. The operational baseline can be used to set budgets and provide support for vulnerability mitigation work. It is understood that these products probably do not meet the future goals, so the focus is on how these products are being used to best conform to the goals as described in the future-looking documents.

Figure 2 describes the overall vision. It starts at its core with the tenets, which are represented by solid rocks that are difficult to move or change. These are surrounded by concepts, which are represented by wood, which is still solid but more flexible than the tenets. The requirements are represented by formal documents, which can be changed easily but still have significant weight attached to them.

Beyond these central ideas are the three layers of documentation, the Target Baseline, the Implementation Baseline, and the Operational Baseline. Each layer is primarily related to and affected by the neighboring layers. The Target Baseline is directly driven by the Requirements, which are a practical expression of the higher-level Concepts and ultimately the Tenets. The Implementation Baseline products are evaluated directly against the Target Baseline’s Technical Profile document requirements. In addition, as products are evaluated, there is a feedback process that can adjust the Target Baseline and the Technical Profile requirements to better align them with current technology. The Operational Baseline relates to the Implementation Baseline for currently fielded products that were not previously evaluated in the Implementation Baseline. These product configurations and operational practices are documented in the Operational Baseline, and

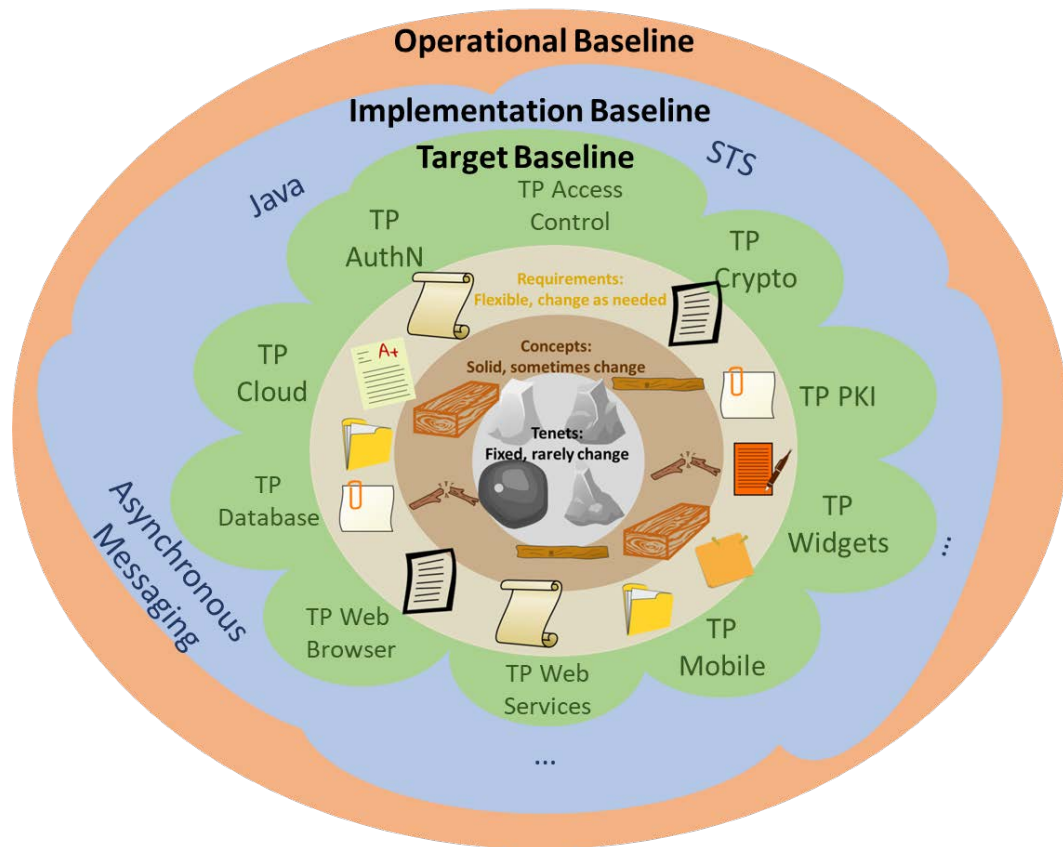


Figure 2. The Vision, from Tenets to Operational Baseline

any shortcomings with respect to Implementation Baseline documents for similar products are highlighted. Mitigations for vulnerabilities are also noted. Often, these are workarounds for missing capability that involve inefficiencies or security risks. By documenting these workarounds, the Implementation Baseline documents have better information about which shortcomings in current products have existing workarounds and which are fundamental problems that will require additional cost or effort. Ultimately, the Operational Baseline and the operational procedures should be driven by the Tenets, Concepts, and Requirements through this process, which keeps the entire enterprise consistent to the extent possible. Shortcomings are documented, workarounds noted, and expected compliance plans and dates are recorded.

Current Status

The current status of the different documents varies by type. The target baseline (Consolidate Enterprise IT Baseline [CEITB]) documents [7] are currently fairly mature and are in their fifth iteration approved on October 1, 2018, as listed in Table 1. The

Scenarios include many different questions about how to perform different mission needs. The basic security model is well-established and documented in a special “Design Technical Profile” called “Application Security Guidelines.” This describes the tenets, key concepts, and high-level requirements for building an ELS system. Many of the core security function documents are mature as well. These “Building Block Technical Profiles” include Authentication, Public Key Infrastructure, Access Control, and Monitoring. These apply across a large number of different capabilities and technologies. “Capability Technical Profiles” are also fairly mature, and include the many technologies and capabilities that build on the core security functions to provide functionality for the enterprise.

The “Capability Profiles” that link the Target Baseline to the Implementation Baseline are still in development. An important question for these documents is what constitutes a capability versus a requirement. The capabilities in these documents must be described at a high enough level that they do not restrict a vendor’s implementation. This

allows for vendor creativity and inclusion of new technologies. However, the capabilities must be defined specifically enough that vendors cannot simply bypass key security requirements by using new and different approaches that are not proven or secure.

The Implementation Baseline contains several documents, and the current version is 3.3 with a release date of 18 January 2018. [8] These documents are listed in Table 2. It can be difficult to get enough information from vendors to assess their products against the fairly detailed security requirements in the Target Baseline Technical Profiles. It is tempting to simply ask the vendors if they meet all the requirements and happily accept a “Yes” answer to all such questions. However, the purpose of these documents is to provide reliable

information about products, and vendors do not always provide such information freely, especially the information about requirements their products do not meet. Feedback to the groups producing target baseline documentation and education of the group writing the Implementation Baseline about current Target Baseline requirements will improve the overall evolution.

The current status of the Implementation Baseline includes a set of documents that partially assess vendor products. The process to perform full assessments is still under development. The need for funding of full-time trained professionals in this area is great.

The final component, the “Operational Baseline,” has not been documented yet. The first step is to

Table 1. CEITB Target Baseline Documentation

#	Technical Profiles	5.0 version	#	Scenarios	5.0 version
1	Application Security Guidelines	9/27/17	1	Access Management	5/11/16
2	Configure IDPS	7/28/18	2	Application Hosting	4/11/16
3	Manage Info - Provide Digital Policy with QoS	5/29/18	3	Application Performance Management	4/11/16
4	Provide Access Control	5/29/18	5	Data Management and Information Exchange	10/21/16
5	Provide Access Control Annexes	5/29/18	6	Data on Human Users	11/14/16
6	Provide Authentication	5/29/18	7	Edge Information Management	5/13/16
7	Provide Automated Info Capture Services	10/20/17	8	Elasticity	10/11/16
8	Provide Cloud Services	8/3/17	9	Enterprise Info. Management	10/19/16
9	Provide Consolidated Storage Services	1/13/16	10	Ground Segment Telem. and Command	10/14/16
10	Provide Cryptographic Services	5/29/18	11	Incident Response	5/16/16
11	Provide Data Mining Services	8/5/17	12	Infrastructure and Application Defense	5/11/16
12	Provide Data/Info/Protocol Mediation Services	8/5/17	13	IT Service Management	12/12/16
13	Provide Database Services	2/5/17	14	Key Management	5/3/16
14	Provide Domain Name Services	5/27/17	15	Leverage Digital Signature	5/11/16
15	Provide Load Balancing	8/15/17	16	Leverage Infrastructure Services	5/17/16
16	Provide Messaging Services	8/4/17	17	Mobile Enterprise	6/28/16
17	Provide Metadata Tagging & Discovery Services	8/5/17	18	Mobile Enterprise Annex 1 AIDC	6/6/17
18	Provide Mobile Ad Hoc Network Services	5/15/18	19	Mobile Enterprise Annex 2 Loc. Services	6/6/17
19	Provide Monitoring Services	9/27/17	20	Mobile Enterprise Annex 3 Wireless	6/6/17
20	Provide Network and Application Defense	8/5/17	21	Mobile Enterprise Annex 4 Device Mgt	6/6/17
21	Provide Operating System Services	8/4/17	22	Mobile Enterprise Annex 5 IoT	6/6/17
22	Provide Public Key Infrastructure Services	8/4/17	24	Network and Precision Timing	11/14/16
23	Provide Presentation Services	8/5/17	25	Resiliency	11/7/16
24	Provide Service Desk Management Services	5/29/18			
25	Provide Streaming Media Services	8/5/17			
26	Provide Virtualization Services	8/4/17			
27	Provide Web Browsing	8/4/17			
28	Provide Web Hosting	5/16/16			
29	Provide Web Services	5/31/18			
30	Provide Widget Services	8/4/17			
31	Provide Ports and Protocol Policy	10/20/17			
32	Provide Satellite Communications	10/4/17			
33	Establish Space Time Information Correlation	9/27/17			
34	Provide Collaboration Services	7/11/18			
35	Provide Endpoint Device Management	5/29/18			
			#	Capability Profiles	5.0 version
			1	Endpoint Management Service (CP)	7/23/18

identify all current products in use. This has been attempted, but it is a considerable effort for a large enterprise, and current results are incomplete. Currently assigned personnel at the operational level do not have time to organize this aspect, and it may have to await staffing for this function. Essential feedback to both the target baseline and implementation baseline will improve the overall continuous improvement of the enterprise IT. It is expected that these documents will be very limited distribution.

Figure 3 shows the relationships between the different types of documentation. The Target Baseline currently has the most internal structure. Of the components of the Target Baseline, the Technical Profiles have the most structure. This reflects the effort put into these categories of documents. It is expected that the Implementation

Baseline and Operational Baseline will be refined further as more work is put into them.

The dashed lines indicate paths of influence between the document types. For example, mission needs identified in scenarios shape the Capability Technical Profiles, the products analyzed for the Implementation Baseline, and the assessment of vendors' future product plans. There is mutual feedback between the capability assessments of the Implementation Baseline and Operational Baseline. Upgrades for the Operational Baseline are influenced by, and can also influence, the core security requirements in the Building Block Technical Profiles. Many other interactions are possible. These help to keep all the documents more cohesive and relevant to each other and to current technology trends and products.

Table 2. CEITB Implementation Baseline Documentation

#	Implementation Baseline Document	3.3 Version
1	Air Force Managed Platforms .NET Baseline	11/30/16
2	Air Force IB 3.3 Executive Summary	11/30/16
3	Air Force Implementation Baseline	11/30/16
4	Air Force Application Services Addendum	11/30/16
5	Air Force Managed Platforms Database Server Baseline	11/30/16
6	Enterprise Level Security (ELS) Capability Addendum	11/30/16
7	Air Force Managed Platforms Enterprise Resource Planning (ERP) Systems	11/30/16
8	Air Force Managed Platforms Java Baseline	11/30/16
9	Air Force Implementation Baseline 3.3 Approval	1/18/17

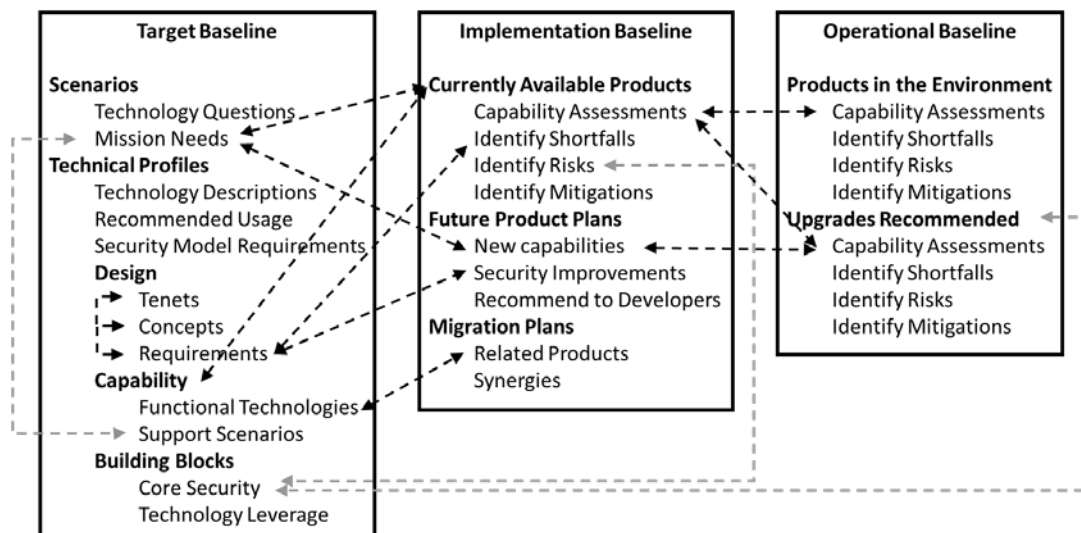


Figure 3. Documentation Hierarchy

In addition to the influence between documents, the periodic discussions that follow these dashed lines help to inform owners of each document type about the other documents that are relevant. This helps to accomplish the following:

- Finding Target Baseline shortfalls in the Implementation Baseline and properly assessing associated risks.
- Finding, understanding, and assessing shortfalls, risks, and mitigations to the Operational Baseline.
- Adding necessary upgrades to the Operational Baseline, or replacing products if upgrades are not available or insufficient.
- Updating the Target Baseline to better align with current products and practices and avoid significant divergence from the commercial state-of-the-art.

Future Plans

The plan for the future is to continue the established process for the Target Baseline, including the periodic review of Scenarios, Technical Profiles, and Capability Profiles. Additions and changes are made as mission needs and technology evolve. Although these documents are fairly mature already, they must constantly be updated to reflect new technology and how it guides the future vision.

As the future becomes the present, we expect to see more products meeting the old requirements. The Implementation Baseline documents will be updated to reflect the current status of products with respect to the original Target Baseline. They will also be assessed against the updated Target Baseline as it evolves. For example, an Implementation Baseline document for a product may contain a history of relevant Target Baseline requirements and when they were first met. This provides information about a vendor's follow-through when promises are made to upgrade and become compliant with Target Baseline requirements.

As new products are purchased using the Implementation Baseline as guidance, these products will evolve toward the Operational Baseline as their configuration, use, and best practices are established.

Thus, with time, the Implementation Baseline and eventually the Operational Baseline will become more mature and populated with documentation.

The process to track technology goals, products, and how we use them reduces the need to do a full assessment from scratch.

Conclusion

The ability to maintain a secure information system is a daunting task. Simple approaches are not up to this task. We propose a systematic way to identify and document future goals, translate these to current actions, and track these over the lifetime of products in the system until they no longer meet operational needs. This requires a dedicated team to work on the future vision, another team to map this vision to currently available products, and a third to document operational procedures for current products. By maintaining these teams and fostering communication between them, it is possible to maintain the collective expertise of an expert. The periodic review and documentation provides the stability of a bureaucracy. The mapping to current products in the Implementation Baseline and Operational Baseline ensures that these ideas track with current best practices of vendors. This approach is currently being developed and implemented, and it is evolving and maturing as more mission needs are raised, more technologies are analyzed, more products are reviewed, and the operational procedures for these products are matured and documented. This paper is part of a body of work for high-assurance enterprise computing using web services [9-15]

Acknowledgments

This work was supported in part by the U.S. Secretary of the Air Force and The Institute for Defense Analyses (IDA). However, the publication of this paper does not indicate endorsement by any organization in the Department of Defense or IDA, nor should the contents be construed as reflecting the official or unofficial position of these organizations or their members.

References

- [1] United States Labor Department, Bureau of Vital Statistics, Occupational Outlook Handbook, Computer and Information Systems Managers, April, 2018, <https://www.bls.gov/ooh/management/computer-and-information-systems-managers.htm> , accessed on 11 October 2018.
- [2] Gino, Francesca and Staats, Bradley, “Why Organizations Don’t Learn,” Harvard Business Review, November 2015. Available at <https://hbr.org/2015/11/why-organizations-dont-learn> .
- [3] Cambridge University Press, Cambridge Dictionary, <https://dictionary.cambridge.org/dictionary/english/bureaucracy> , accessed on 11 October 2018.
- [4] Johnson, Ronald N. and Libecap, Gary D., The Federal Civil Service System and The Problem of Bureaucracy, University of Chicago Press, January 1994. Available at <http://www.nber.org/chapters/c8632.pdf> .
- [5] Opara-Martins et al., “Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective,” Journal of Cloud Computing: Advances, Systems and Applications (2016) 5:4. DOI 10.1186/s13677-016-0054-z
- [6] Kevin E. Foltz and William R. Simpson, 2016. Proceedings of The 20th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI, Enterprise Level Security – Basic Security Model, Volume I, WMSCI 2016, Orlando, Florida, 8–11 March 2016, pp. 56–61.
- [7] Secretary of the Air Force, Office of the Chief Information Office, Information Dominance, Air Force Chief Technology Officer, https://intelshare.intelink.gov/sites/afceit/tb_release/s/_layouts/15/start.aspx#/SitePages/Current%20Release.aspx, Target Baseline Release, 1 October 2018, Not available to all but document distribution is not limited.
- [8] Air Force Lifecycle Management Center Maxwell AFB-Gunter Annex, Alabama, Program Executive Officer Command, Control, Communications, Intelligence and Networks (PEO C3I&N), Air Force Implementation Baseline Documents, Version 3.3, Not Available to all, Distribution Limited, <https://intelshare.intelink.gov/sites/ib/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fb%2fShared%20Documents%2fIB%5f3%2e3&FolderCTID=0x012000F3C89072A720F3458AA913A8E8C84E3F>, 18 January 2017.
- [9] William R. Simpson, and Kevin E. Foltz, 2017. Lecture Notes in Engineering and Computer Science, Assured Identity for Enterprise Level Security, Proceedings of the World Congress on Engineering, July 2017, Imperial College, London, pp. 440–445,
- [10] William R. Simpson, and Kevin E. Foltz, 2017. Enterprise Level Security: Insider Threat Counter-Claims, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2017, 25–27 October, 2017, San Francisco, USA, pp. 112–117.
- [11] William R. Simpson and Kevin E. Foltz, 2017. Proceedings of the 22nd International Command and Control Research and Technology Symposium (ICCRTS), Escalation of Access and Privilege with Enterprise Level Security, Los Angeles, CA. September 2017, pp. TBD.
- [12] William R. Simpson and Kevin E. Foltz, 2017. Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017), Volume 1, pp. 177–184, Porto, Portugal, 25–30 April, 2017, Enterprise Level Security with Homomorphic Encryption, SCITEPRESS – Science and Technology Publications.
- [13] Kevin Foltz, and William R Simpson, 2016. “Enterprise Considerations for Ports and Protocols, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2016, 19–21 October, 2016, San Francisco, USA, pp.124–129.
- [14] Simpson, William R., CRC Press, 2016. Enterprise Level Security – Securing Information Systems in an Uncertain World, by Auerbach Publications, ISBN 9781498764452, May 2016, 397 pp.
- [15] Kevin E. Foltz and William R. Simpson, 2016. Wessex Institute, Proceedings of the International Conference on Big Data, BIG DATA 2016, Access and Privilege in Secure Big Data Analysis, 3–5 May 2016, Alicante, Spain, pp. 193–205.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YY) 00-11-18		2. REPORT TYPE Non-Standard		3. DATES COVERED (From – To)	
4. TITLE AND SUBTITLE Managing Information System Technology Changes across an Enterprise				5a. CONTRACT NUMBER HQ0034-14-D-0001	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBERS	
6. AUTHOR(S) Kevin E. Foltz, William R. Simpson				5d. PROJECT NUMBER BC-5-2283	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882				8. PERFORMING ORGANIZATION REPORT NUMBER NS D-10378	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Frank P. Konieczny USAF HQ USAF SAF/CIO A6 United States Air Force SAF-CIO A6, 1800 Air Force Pentagon, Washington DC 20330-0001				10. SPONSOR'S / MONITOR'S ACRONYM	
				11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT This draft has not been approved by the sponsor for distribution and release.					
13. SUPPLEMENTARY NOTES Project Leader: William R. Simpson					
14. ABSTRACT The goal of information management systems in an enterprise is to make the right information available to the right entities at the right times and in the right formats. The standard approach is to purchase a new system to meet current needs. Patches, work-arounds, and added components satisfy the changing future needs while creating an increasingly complex system, and operational capability slowly degrades over time as complexity builds. The system is then rebuilt from the ground up, at great cost and inconvenience, and the cycle repeats. This paper describes an approach for constant change. Instead of building the best system possible based on today's needs, only to replace it in the future, the goal is a system that is capable of evolving toward a better future in a consistent and directed way. This prevents one-off fixes from lingering, and it keeps the distributed decision-making process aligned toward a common enterprise goal. Components not consistent with future goals are identified and scheduled for replacement. Current practices chosen for expedience are assigned expiration dates to prevent them from becoming solidified in the future architecture. The replacement cycle is applied to components of the system instead of the entire system. This stops the cycle of complete replacements by allowing constant change, which reduces overall cost and maintains a more consistent operational capability.					
15. SUBJECT TERMS Enterprise level security, target baseline, implementation baseline, operational baseline, information technology					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Unlimited	18. NUMBER OF PAGES 9	19a. NAME OF RESPONSIBLE PERSON Frank P. Konieczny
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include Area Code) 703-697-1308

