

# SYSTEMS ARCHITECT

## Procedure Guide



This procedure guide is not intended to encompass all facets of all the tasks a Systems Architect would potentially be responsible for in their position. It is a working draft subject to revision based upon community feedback.

PG-2013-001  
Version 1 Release 1  
10 JANUARY 2014

This page is intentionally left blank.

**DOCUMENT REVISION HISTORY**

Version Release	Date	Description
V0 R1	10 JANUARY 2014	Initial DRAFT release.

## TABLE OF CONTENTS

<b>DOCUMENT REVISION HISTORY.....</b>	<b>iii</b>
<b>TABLE OF CONTENTS .....</b>	<b>iv</b>
<b>TABLE OF TABLES.....</b>	<b>viii</b>
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1. Document Organization .....	1
1.2. Purpose.....	2
1.3. Scope.....	2
1.4. How To Use This Document .....	2
<b>2. THE METHODOLOGY-BASED APPROACH.....</b>	<b>3</b>
<b>3. ANALYZE USER NEEDS TO PLAN ARCHITECTURE.....</b>	<b>5</b>
3.1. Training.....	5
3.2. Implementation .....	5
3.2.1 Task: Determine the IA Architecture.....	5
3.2.2 Task: Determine the Appropriate DoD Trust Model.....	5
3.2.3 Task: Determine Intended Use of Architecture .....	6
3.2.4 Task: Identify the Business Goals.....	7
3.2.5 Task: Categorize the System Against the Appropriate DoD Information System (IS) Category.....	7
3.2.6 Task: Identify Risk Mitigation Factors .....	8
3.2.7 Task: Analyze Constraints that will Affect Design .....	8
<b>4. DESIGN SYSTEM ARCHITECTURE .....</b>	<b>11</b>
4.1. Training.....	11
4.2. Implementation .....	11
4.2.1 Task: Determine the Scope of the Architecture .....	11
4.2.2 Task: Scoping Architectures to be “Fit-for-Purpose” .....	12
4.2.3 Task: Determine a DoDAF Viewpoint and Model .....	14
<b>5. WRITE SPECIFICATIONS &amp; DOCUMENT DEVELOPMENT .....</b>	<b>17</b>
5.1. Training.....	17
5.2. Implementation .....	17
5.2.1 Task: Collect, Organize, Correlate, and Store Architectural Data.....	17
5.2.2 Task: Document Results in Accordance with Decision-Maker Needs .....	18
<b>6. SPECIFY POWER SUPPLY REQUIREMENTS.....</b>	<b>19</b>

6.1.	Training.....	19
6.2.	Implementation .....	19
6.2.1	Task: Require the Use of a Dedicated Circuit .....	19
6.2.2	Task: Require the Use of Surge Suppressors.....	19
6.2.3	Task: Require the Install of a Backup Power Supply .....	19
6.2.4	Task: Require the Use of Redundant Components.....	20
<b>7.</b>	<b>EVALUATE INTERFACE BETWEEN HARDWARE AND SOFTWARE....</b>	<b>21</b>
7.1.	Training.....	21
7.2.	Implementation .....	21
7.2.1	Task: Implement Multiprocessing .....	21
7.2.2	Task: Implement Process Management .....	21
7.2.3	Task: Implement Preemptive Multitasking.....	22
7.2.4	Task: Determine Whether to Run Processes in a Running State, Ready State, or Blocked State .....	22
7.2.5	Task: Utilize Thread Management.....	22
7.2.6	Task: Enforce Process Isolation.....	22
7.2.7	Task: Implement Memory Management.....	23
7.2.8	Task: Avoid Buffer Overflow .....	23
7.2.9	Task: Avoid Memory Leaks .....	23
7.2.10	Task: Implement Input/Output Device Management .....	23
<b>8.</b>	<b>DOCUMENT DESIGN SPECIFICATIONS .....</b>	<b>24</b>
8.1.	Training.....	24
8.2.	Implementation .....	24
8.2.1	Task: List the Architecture Products That Will be Developed .....	24
8.2.2	Task: Summarize the System-Level Technical Certifications Obtained .....	25
8.2.3	Task: Create a Technical Schedule and Schedule Risk Analysis .....	25
8.2.4	Task: List and Summarize the Program Oversight and Management Systems .....	27
8.2.5	Task: Diagram the Process for How the Program Plans to Manage Engineering .....	27
8.2.6	Task: Indicate Roles, Responsibilities, and Authorities Within the Risk Management Process .....	28
8.2.7	Task: Provide a Listing of the Current System-Level Technical Risks.....	28
8.2.8	Task: Provide Planned Program Office Organization Structure.....	28
8.2.9	Task: Summarize the Program's Technical Staffing Plan .....	29
8.2.10	Task: Describe Relationships with External Technical Organizations.....	29
8.2.11	Task: Identify Technical Performance Measures and Metrics .....	30
8.2.12	Task: Summarize Technical Activities and Products .....	30

8.2.13	Task: Document Requirements Management and Change Process.....	31
8.2.14	Task: Summarize Plans for Conducting Technical Review .....	31
8.2.15	Task: Identify Engineering Tools the Program Plans to Use.....	31
<b>9.</b>	<b>ENSURE COMPATIBILITY OF SYSTEM COMPONENTS .....</b>	<b>33</b>
9.1.	Training.....	33
9.2.	Implementation .....	33
9.2.1	Task: Understand CPU Architecture .....	33
9.2.2	Task: Understand Operating System Architecture .....	34
9.2.3	Task: Apply Security Policy .....	34
9.2.4	Task: Know How the Trusted Computing Base Works .....	34
9.2.5	Task: Secure the Security Kernel.....	35
<b>10.</b>	<b>EVALUATE CURRENT OR EMERGING TECHNOLOGIES .....</b>	<b>36</b>
10.1.	Training.....	36
10.2.	Implementation .....	36
10.2.1	Task: Use the Defense Acquisition Guide (DAG).....	36
<b>11.</b>	<b>DEVELOP A SYSTEM SECURITY CONTEXT .....</b>	<b>41</b>
11.1.	Training.....	41
11.2.	Implementation .....	41
11.2.1	Task: Implement a Security Model.....	41
11.2.2	Task: Conduct an Assurance Evaluation .....	42
11.2.3	Task: Implement Security Modes of Operation Used in Mission Assurance Category (MAC) Systems.....	42
11.2.4	Task: Understand the Common Criteria (CC) .....	44
<b>12.</b>	<b>ADDRESS DOD ENGINEERING REQUIREMENTS .....</b>	<b>45</b>
12.1.	Training.....	45
12.2.	Implementation .....	45
12.2.1	Task: Utilize the Defense Acquisition Management System .....	45
12.2.2	Task: Utilize the Defense Acquisition Guidebook (DAG) .....	46
<b>13.</b>	<b>IDENTIFY PROTECTION NEEDS.....</b>	<b>47</b>
13.1.	Training.....	47
13.2.	Implementation .....	47
13.2.1	Task: Plan a Security Design with Risk in Mind.....	47
13.2.2	Task: Implement Access Control.....	47
<b>14.</b>	<b>PROVIDE INPUT TO THE IA C&amp;A PROCESS .....</b>	<b>50</b>
14.1.	Training.....	50

14.2.	Implementation .....	50
14.2.1	Task: Identify the DIACAP's Purpose and its Importance in Protecting DoD Information and Information Systems .....	50
14.2.2	Task: Identify the Interrelationship of the DIACAP and its Implementation Tools .....	50
14.2.3	Task: Understand Enterprise Risk Management.....	51
14.2.4	Task: Assign DoD MAC and Confidentiality Level.....	52
14.2.5	Task: Implementing IA Controls .....	54
14.2.6	Task: Explain DIACAP Enterprise Governance.....	55
14.2.7	Task: Identify Key Players Involved in DIACAP Execution .....	55
14.2.8	Task: Identify the DIACAP Activities.....	56
14.2.9	Task: Identify the DIACAP Package Components.....	56
14.2.10	Task: Understand how IA C&A is Planned and Initiated.....	57
14.2.11	Task: Understand how IA Controls are Validated and Assigned .....	57
14.2.12	Task: Understand how Determination and C&A Decision is Made.....	58
14.2.13	Task: Understand How to Maintain Authorization to Operate.....	58
14.2.14	Task: Understand Decommissioning of a DoD Information System .....	59
<b>15.</b>	<b>ENSURE CONSISTENCY WITH DOD ARCHITECTURE .....</b>	<b>60</b>
15.1.	Training.....	60
15.2.	Implementation .....	60
15.2.1	Task: Ensure all IA and IA-enabled IT Products are Validated and Certified in Accordance with the Common Criteria (CC) .....	60
<b>16.</b>	<b>PERFORM TECHNICAL REVIEW .....</b>	<b>63</b>
16.1.	Training.....	63
16.2.	Implementation .....	63
16.2.1	Task: Summarize Plans for Conducting Technical Review .....	63
16.2.2	Task: List and Describe Planned or Established Artifacts.....	65
16.2.3	Task: Provide a Configuration Management (CM)/Control Process Description.....	65
<b>17.</b>	<b>PRIORITIZE CAPABILITIES AFTER A CATASTROPHY.....</b>	<b>67</b>
17.1.	Training.....	67
17.2.	Implementation .....	67
17.2.1	Task: Use the Trusted Recovery Methodology to Deter, Detect, and Reduce Impacts to Mission and Functions .....	67
17.2.2	Task: Use Reconstitution Tactics.....	68
17.2.3	Task: Prioritize Essential System Capabilities .....	68
17.2.4	Task: Implement Software Escrow .....	69

<b>APPENDIX A – NICE TO JCT&amp;CS CROSSWALK .....</b>	<b>A-1</b>
<b>APPENDIX B – REFERENCES .....</b>	<b>B-1</b>
<b>APPENDIX C – TRAINING RESOURCES IN THE DOD .....</b>	<b>C-1</b>
<b>APPENDIX D – TRAINING RESOURCES .....</b>	<b>D-1</b>
<b>APPENDIX E – SUPPORT AND POC LIST .....</b>	<b>E-1</b>
<b>APPENDIX F - ACRONYM LIST.....</b>	<b>F-1</b>

## **TABLE OF TABLES**

Table 8-1: Technical Certifications .....	25
Table 8-2: Sample Engineering Tools .....	31
Table 16-1: Sample Technical Review Table.....	64
Table A-1: NICE to JCT&CS KSA Crosswalk .....	A-1
Table C-1: Training Course List .....	C-1
Table F-1: Acronym List .....	F-1

## **TABLE OF FIGURES**

Figure 4-1: Establishing the Scope for Architecture Development .....	13
Figure 4-2: Mission Outcomes Supported by Architectures.....	14
Figure 4-3: DoDAF Viewpoints and Models.....	16
Figure 8-1: Detailed Technical Schedule.....	26
Figure 10-1: Technical Management Processes .....	38
Figure 14-1: Choosing the Appropriate MAC Level.....	53
Figure 14-2: Choosing the Appropriate Confidentiality Level.....	54
Figure 14-3: DIACAP Package Components .....	57
Figure 16-1: Sample Process Diagram .....	65



## 1. INTRODUCTION

This Systems Architect Procedure Guide is developed by the Defense Information Systems Agency (DISA) in support of providing the entire Department of Defense (DoD) Systems Architect community with a supplemental source on how to approach the tasks which make up the Systems Architect mission set. This procedure guide is not intended to encompass all facets of all the tasks a Systems Architect would potentially be responsible for in their position. It is a working draft subject to revision based upon community feedback. Systems Architects construct the basic structure of the computer system, defining the significant foundational design features and requisites that provide the framework for all that follow. They define the user's vision for the system's needs, functions, and the path of its evolution. They strive to maintain the integrity of that vision as it evolves during detailed design and implementation.

This guide represents knowledge based on the functions in the *USCYBERCOM Concept of Operations (CONOPS) Joint Cyberspace Training and Certification Standards (JCT&CS)*, also known as Qualification Standards (QS), and serves as a general basis for further policies and procedures to be executed upon. Each site or enclave<sup>1</sup> will have additional measures or requirements, but each individual in the role of a Systems Architect can benefit from the information covered in this guide.

### 1.1. Document Organization

This document is organized in the following manner:

- Section 1 provides an introduction, outlines the purpose, scopes what is covered within, and describes how to use this document.
- Section 2 describes the methodology-based approach to architecture development.
- Sections 3-17 identify the job functions of the Systems Architect.
- Appendix A provides a National Initiative for Cybersecurity Education (NICE) to JCT&CS Knowledge, Skills, and Abilities (KSA) crosswalk.
- Appendix A provides a list of references used to derive the material in this guide.
- Appendix B provides the Qualification Standards for the Systems Architect<sup>2</sup>.
- Appendix C identifies DoD training resources.
- Appendix D identifies additional training resources.

---

<sup>1</sup> "An enclave is the collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security." *Enclave Security Technical Implementation Guide*, Version 4, Release 3, 28 January 2011

<sup>2</sup> *USCYBERCOM Concept of Operations (CONOPS) Joint Cyberspace Training and Certification Standards (JCT&CS) V.1.2*, 7 February 2012

- Appendix E provides a form to maintain a list of operational contacts and a list of support contacts.
- Appendix F provides the list of acronyms and their definitions as used in this guide.

## 1.2. Purpose

The Systems Architect's role is to analyze needs of users; design and document system architecture and its development process; specify requirements based on system performance; advise on topics such as project costs, design concepts, or design changes; and develop a system security context and provide input on security requirements. The Systems Architect should also be able to document and address DoD information systems' IA architecture and systems security engineering requirements throughout the acquisition life-cycle. Once an information system is in place, a Systems Architect may need to conduct security reviews and identify gaps in security architecture and subsequently assist in developing a risk management plan.

In addition to the responsibilities outlined above, the Systems Architect also contributes to the DoD's task to accept a Risk Management Program that addresses these five essential competencies within the DoD IA Program described in *DoDI 8500.2, Information Assurance (IA) Implementation*:

- The ability to assess security needs and capabilities.
- The ability to develop a purposeful security design or configuration.
- The ability to implement required controls or safeguards.
- The ability to test and verify.
- The ability to manage changes to an established baseline in a secure manner.

## 1.3. Scope

This guide is limited to the actions required for a Systems Architect to successfully execute their functions in the DoD environment.

## 1.4. How To Use This Document

This guide was designed to be used in a self-paced environment without the use of hands-on applications. It provides information to assist a variety of anticipated audiences.

## 2. THE METHODOLOGY-BASED APPROACH

### **The Methodology-Based Approach to Architecture Development**

The Qualification Standards described in this document are drawn from a variety of credible sources, including the methodology-based approach to architecture development described in this section. The methodology-based approach to Architectural Description<sup>3</sup> development within the DoD draws on the methodology described in DoD Architecture Framework Version 2.0 and highlights its use in a data-driven, net-centric architecture development environment. This methodology represents best practices that have evolved over time, and can be utilized in conjunction with, or as a replacement for other methodologies, as described below.

Generally speaking, knowledge is gained through the acquisition of, and effective use of information organized from data for a particular purpose. An architecture development methodology specifies how to derive relevant information about an enterprise's processes and business or operational requirements, and how to organize and model that information. Architecture methods describe consistent and efficient ways to collect data, organize the data in a particular grouping or structure, and store collected data for later presentation and use in decision-making processes. A methodology also provides a means for replicating the steps taken to create an Architectural Description for a specific purpose later by another person or team with the expectation of achieving similar results. In turn, through utilization of a method, it is possible to compare Architectural Descriptions created under the same, or similar methods, evaluate how disparate Architectural Descriptions can be linked to provide a higher-level picture of a process or capability, and analyze the impact of future change. These analyses can include:

**Static Analyses** – which could include capability audit, interoperability analysis, or functional analysis. These analyses are often performed using simple analysis tools such as paper-based comparisons and database queries.

**Dynamic Analyses** – sometimes referred to as executable models, these analyses typically examine the temporal, spatial, or other performance aspects of a system through dynamic simulations. For example, these analyses might be used to assess the latency of time sensitive targeting systems or conduct traffic analyses on deployed tactical networks under a variety of loading scenarios.

**Experimentation** – the use of tactical capability requirements, such as the Coalition Warrior Interoperability Demonstration (CWID), and various battle labs to provide the ability to conduct human-in-the-loop simulations of operational activities. Differing

---

<sup>3</sup> Architectural Description is an iterative and unique process, in that every Architectural Description is different in that architecture creation serves a specific purpose, and is created from a particular viewpoint; serving different requirements, necessitating different types of views to represent the collected data; representative of a 'snapshot in time'; changeable over time as requirements become more focused or additional knowledge about a process or requirement becomes known.

degrees of live versus simulated systems can be deployed during these experiments and there is a high degree of control over the experiment variables. These can be used for a variety of purposes.

The DoDAF 6-step architecture development process described throughout this document is a generic, time-tested method, which can be utilized, in a wide range of architectural requirements through relatively simple adaptation. The examples described within the steps provide information on customization of the generic method for use in major departmental functions and operations.

**Note:** The methodology described is also applicable to development of Service Oriented Architecture (SOA)-based architectures. The steps described in the methodology, together with the requirements of the toolset, techniques and notation desired, should be considered together when defining a SOA. The Service Viewpoint provides specific models that are useful for services-specific data collection, presentation models, and documents that describe services.

The utilization of the information contained in Architectural Data and Models and the DoDAF Meta-Model (DM2) Physical Exchange Specifications (PES) are useful even when utilizing another method and provides the information needed for use in developing an Architectural Description. When utilizing another method, reference to this methodology can ensure adherence to the principles described in DoDAF V2.0, to maximize the potential for reuse of essential data, and also to ensure conformance with DoDAF V2.0.

### 3. ANALYZE USER NEEDS TO PLAN ARCHITECTURE

**Qualification Standard:** Analyze user needs and requirements to plan system architecture.<sup>4</sup>

#### 3.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the Qualification Standard listed in the title:

[https://powhatan.iie.disa.mil/specialty\\_courses/](https://powhatan.iie.disa.mil/specialty_courses/).

#### 3.2. Implementation

The IA architecture is an abstract expression of IA solutions that assigns and portrays IA roles and behavior among a set of IT assets, and prescribes rules for interaction and interconnection.

##### 3.2.1 Task: Determine the IA Architecture

An IA architecture may be expressed at one of three levels:

- DoD information system-wide
- DoD Component-wide
- Defense-wide

DoD Component-wide and Defense-wide IA architectures provide a uniform and systematic way to assess and specify IA across multiple, interconnecting DoD information systems, and to ensure that they take advantage of supporting IA infrastructures.

##### 3.2.2 Task: Determine the Appropriate DoD Trust Model<sup>5</sup>

Secure information sharing between the Department of Defense (DoD) and its external partners requires Public Key Infrastructure (PKI) interoperability. Like the DoD, many Federal Agencies and DoD partners have implemented a PKI to secure their applications and networks. In the past, these external PKIs were designed to operate independently. Internal policies, technical challenges and vendor selection have all contributed to these different identity management and information protection solutions.

Homeland Security Presidential Directive (HSPD)-12, Federal Information Processing Standards (FIPS)-201, and the Federal Bridge Certificate Authority (FBCA) have been implemented to synchronize identity management and information protection across the

---

<sup>4</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

<sup>5</sup> JITC [http://jitc.fhu.disa.mil/pki/pke\\_lab/partner\\_pki\\_testing/partner\\_pki\\_status.html](http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html)

federal government. These initiatives aid the federal government and private industry in building PKI based solutions that interoperate moving forward.

DoD External Interoperability Plan, version 1.0 specifies the process by which an external PKI can be approved to interoperate with the DoD PKI. The process differs according to the classification of the external PKI:

- **Category I** - U.S. Federal Agency PKIs.
- **Category II** - Non-Federal Agency PKIs cross-certified with the FBCA or PKIs from other PKI Bridges that are cross-certified with the FBCA.
- **Category III** - Foreign, Allied, or Coalition Partner PKIs or other PKIs.

The interoperability testing phase of this process is conducted by the Joint Interoperability Test Command Public Key-Enabled (PKE) Lab according to the DoD PKI Interoperability Test Plan, version 2.0. Two key trust models are tested:

**Direct Trust Model** - The DoD PKE test application will be required to trust the root certificate of the target PKI and have access to its revocation information in order to determine the validity of the target PKI's certificates.

**Cross Certificate Trust Model** - The DoD PKI and the target PKI will each issue a certificate to a Certification Authority (CA) in the other PKI, or a third party CA trusted by both, creating a cross-certificate pair or pairs providing bi-directional trust. Trust can also be one-way if only one CA signs a certificate for the other CA.

More detailed information can be found at <http://iase.disa.mil/pki-pke/interoperability/index.html>.

### 3.2.3 Task: Determine Intended Use of Architecture

As described in the *DoD Deputy Chief Information Officer's DoD Architecture Framework Version 2.0*, it is necessary to determine the intended use of the architecture as part of the 6-step Architecture Development Process:

- Define the purpose and intended use of the architecture
- How the Architectural Description effort will be conducted
- The methods to be used in architecture development
- The data categories needed
- The potential impact on others
- The process by which success of the effort will be measured in terms of performance and customer satisfaction

This information is generally provided by the process owner to support architecture development describing some aspect of their area of responsibility.

The 6-step Architecture Development Process is explained in detail throughout the Sections in this guide.

#### 3.2.4 Task: Identify the Business Goals

Considering the business goals and constraints of the information system's owner is an essential part of designing an IT system or network. One must collect a thorough analysis of the owner's business objectives. They must state an overall goal of the design project that highlights the purpose of the new IS. These goals and constraints will help a Systems Architect formulate a better plan and have a successful outcome upon completion of the project. An important part of identifying the business goals is ensuring the IS fits into a DoD IS category. Once the business goals have been identified, they are incorporated into the Design Document outlined in section 8 of this document.

#### 3.2.5 Task: Categorize the System Against the Appropriate DoD Information System (IS) Category

According to *DoDI 8510, DIACAP*, DOD categorizes information systems into four major categories: AIS, Enclave, Outsourced IT-based Process, and Platform IT Interconnection. DoD Information Assurance Certification & Accreditation Process (DIACAP) is implemented for each these types utilizing a lifecycle centric model<sup>6</sup>.

**Automated Information System (AIS):** A product or deliverable of an acquisition program performing clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition.

**Enclave:** A collection of computing environments connected via one or more internal networks, under the control of a single authority and security policy, including personnel and physical security.

**Outsourced IT-based Process:** A general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services.

**Platform IT Interconnection:** Computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real-time to the mission performance of special purpose systems.

---

<sup>6</sup> Lifecycle centric model - The systems development life cycle (SDLC), also referred to as the application development life-cycle, is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system. The systems development life-cycle concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.

### 3.2.6 Task: Identify Risk Mitigation Factors<sup>7</sup>

Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of missions and business functions. A significant challenge for organizations is to determine the most cost-effective, appropriate set of security controls, which if implemented and determined to be effective, would mitigate risk while complying with security requirements defined by applicable federal laws, Executive Orders, regulations, policies, directives, or standards (e.g., FISMA, OMB Circular A-130, HSPD-12, FIPS Publication 200). There is no one correct set of security controls that addresses all organizational security concerns in all situations. Selecting the most appropriate set of security controls for a specific situation or information system to adequately mitigate risk is an important task that requires a fundamental understanding of organizational mission/business needs while demonstrating due diligence. Selecting, implementing, and maintaining an appropriate set of security controls to adequately protect the information systems employed by organizations requires strong collaboration with system owners to understand ongoing changes to missions/business functions, environments of operation, and how the systems are used. The baseline Information Assurance levels are described in the *DoD Instruction 8500.2, Information Assurance (IA) Implementation, Enclosure 4*.

### 3.2.7 Task: Analyze Constraints that will Affect Design<sup>8</sup>

#### **Scalability**

In order to analyze constraints that will affect design, a Systems Architect must figure out how much growth a design must support, or its scalability. For example, users will need to be added, applications will need to be installed, and additional external network connections may increase at a rapid rate. The Systems Architect will need to understand how much the network is expected to expand over the next five years.

Generally, scalability deals with the amount of data to be processed, stored, transmitted, and changed over time. A system that can scale appropriately will ingest, normalize, process, and stage information within the timeframes required to service known user requirements. This can be quantified as either a function of end user experience (screen refresh time), or the time between data receipt and availability of analytic results to a user.

Systems tend to scale flat, linearly, or exponentially, and understanding how the addition of new data or new analytics will impact time to process, overall data capacity, and end user experiences. These are all important to ensure that small scale prototypes or initial testing can be expected to represent actual system performance in production.

#### **Availability**

---

<sup>7</sup> *DoD Instruction 8500.2, Information Assurance (IA) Implementation*, 6 February 2003

<sup>8</sup> Cisco Systems, *Top Down Network Design, A Systems Analysis Approach to Enterprise Network Design*



Availability refers to the amount of time a network is available to users and is a critical goal for design customers. It can be expressed as a percent uptime per year, month, week, day, or hour. It is a measure of how much time the system is operational. Redundancy is a solution to the goal of availability. Resiliency refers to the amount of stress a system can handle and how quickly it can rebound from the problem. A system that has good resiliency usually has good availability. Recoverability specifies how easily and in what timeframe a system can recover from a problem. All of these components of Availability are mechanisms a System Architect will need to keep in mind when planning a systems design. There is a major difference between an uptime of 99.70% (represents a downtime of 30 minutes per week) and 99.95% (represents a downtime of 5 minutes per week). For example, it is acceptable for a system only used from 8am-5pm to be unavailable on weekends and overnights to do database backups, offline storage, and systems maintenance. However, a system that is used 24 hours per day, 7 days per week, 365 days per year will need more robust and expensive measures in place to provide availability.

### **Cost of Downtime**

The most important goal of Availability should be to keep mission-critical applications running with little to no downtime. The preferred method to understand availability requirements is to specify a cost of downtime. Downtime in the DoD is measured in regards to an increase in mission effectiveness and a decrease in mission degradation.

### **Mean Time Between Failure and Mean Time to Repair (MTBF and MTTR)**

A Systems Architect can use MTBF and MTTR to calculate availability goals when the customer wishes to indicate precise periods of uptime and downtime, as opposed to a simple percent uptime value.

MTBF estimates how long a system will last before it fails. It is also known as mean time between service outage, or MTBSO. MTTR estimates how long it will take to repair a system. When specifying availability using MTBF and MTTR, the equation to use is as follows:

$$\text{Availability} = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

Using this availability equation allows a customer to clearly state the acceptable frequency and length of outages.

### **Accuracy**

The overall goal for accuracy is that the data received at the destination must be the same as the data sent by the source. Typical causes of data errors include power surges or spikes, impedance mismatch problems, poor physical connections, failing devices, and noise cause by electrical machinery. Sometimes software bugs can cause data errors also, though software problems are a less common cause of errors than physical-layer problems. Frames that have an error must be retransmitted, which has a negative effect on throughput. In the case of IP networks, the Transmission Control Protocol (TCP) provides retransmission of data.

### **Efficiency**

Efficiency is a measurement of how effective an operation is in comparison to the cost in effort, energy, time, or money. Efficiency specifies how much overhead is required to produce a required outcome. It also provides a useful way to describe performance.

DRAFT

## 4. DESIGN SYSTEM ARCHITECTURE

**Qualification Standard:** Design system architecture or system components required to meet user needs.<sup>9</sup>

### 4.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the Qualification Standard listed in this section:

[https://powhatan.iie.disa.mil/specialty\\_courses/](https://powhatan.iie.disa.mil/specialty_courses/).

### 4.2. Implementation

#### 4.2.1 Task: Determine the Scope of the Architecture

According to the *DoD Architecture Framework version 2.0*, the architecture scope defines the boundaries that establish the depth and breadth of the Architectural Description and establish the architecture's problem set, helps define its context, and defines the level of detail required for the architectural content. While many architecture development efforts are similar in their approach, each effort is also unique in that the desired results or effect may be quite different. As an example, system development efforts generally focus first on process change, and then concentrate on those automated functions supporting work processes or activities. In addition to understanding the process, discovery of these 'system functions' is important in deciding how to proceed with development or purchase of automation support.

Information collected for Architectural Descriptions describing services is similar to information collected for Architectural Descriptions describing systems. For describing services, Architectural Description will collect additional information concerning subscriptions, directory services, distribution channels within the organization, and supporting systems/communications web requirements. Similar situations occur with Architectural Description development for joint operations.

Joint capabilities are defined processes with expected results, and expected execution capability dates. The Architectural Descriptions supporting the development of these types of capabilities usually require the reuse of data already established by the military Services and Agencies, are analyzed, and configured into a new or updated process that provides the desired capability. Included are the processes needed for military service and/or agency response, needed automation support, and a clear definition of both desired

---

<sup>9</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

result and supporting performance measures (metrics). These types of data are presented in models<sup>10</sup>.

The important concept for this step is the clarity of scope of effort defined for the project that enables an expected result. The process owner has the primary responsibility for ensuring that the scoping is correct, and that the project can be successfully completed. Clarity of scope can better be determined by defining and describing the data to be used in the proposed Architectural Description in advance of the creation of views that present desired data in a format useful to managers. Early identification of needed data, particularly data about the Architectural Description itself, the subject-matter of the proposed Architectural Description, and a review of existing data from COIs, can provide a rich source for ensuring that Architectural Descriptions, when developed, are consistent with other existing Architectural Descriptions. It also ensures conformance with any data-sharing requirements within the Department or individual COIs, and conformant with the DM2.

An important consideration beginning with this and each subsequent step of the architecture development process is the continual collection and recording of a consistent, harmonized, and common vocabulary. The collection of terms should continue throughout the architecture development process. As architectural data is identified to help clarify the appropriate scope of the architecture effort, vocabulary terms and definitions should be disambiguated, harmonized, and recorded in a consistent AV-2 process documented in the “DoDAF V2.0 Architecture Development Process for the DoDAF-described Models” Microsoft Project Plan. Analysis of vocabularies across different Architectural Descriptions with similar scope may help to clarify and determine appropriate Architectural Description scope. Specific examples of data identification utilizing the AV-2 Data Dictionary construct are found in the DoDAF Journal.

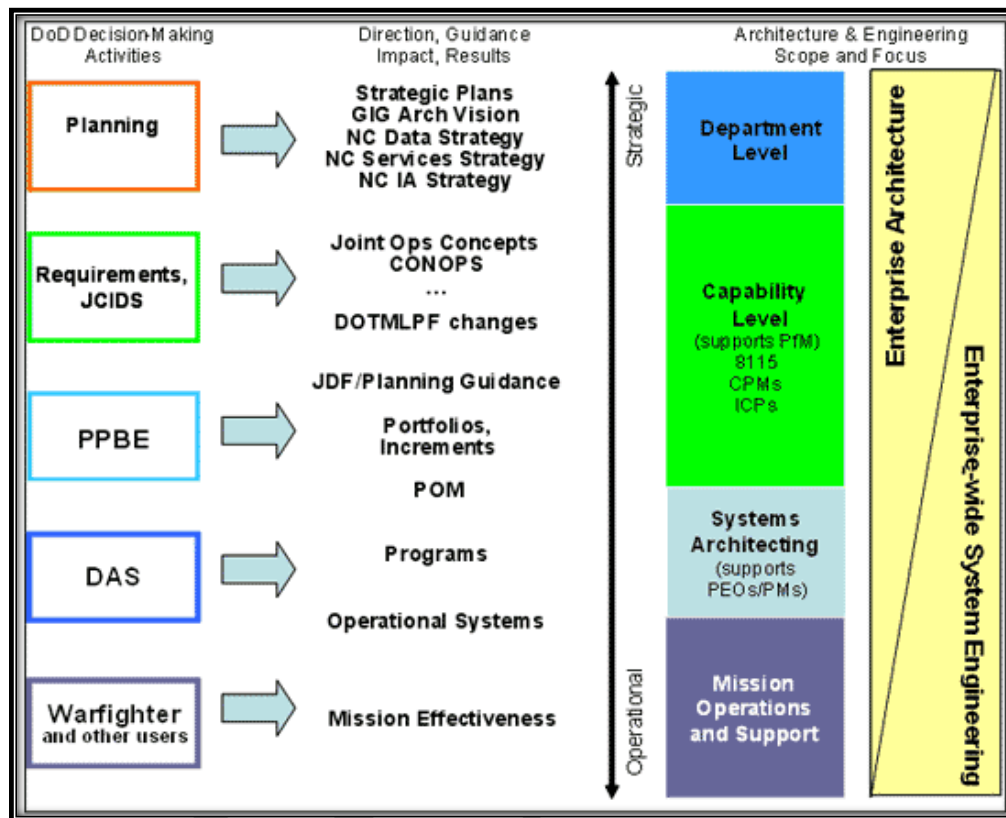
#### 4.2.2 Task: Scoping Architectures to be “Fit-for-Purpose”

Establishing the scope of an architecture is critical to ensuring that its purpose and use are consistent with specific project goals and objectives. The term “Fit-for-Purpose” is used in DoDAF to describe an architecture (and its views) that is appropriately focused. An appropriately focused architecture responds to the stated goals and objectives of the process owner, is useful in the decision-making process, and responds to internal and external stakeholder concerns. Meeting intended objectives refers to those actions that either directly support customer needs or improve the overall process undergoing change. The architect is the technical expert who translates the decision maker’s requirements into a set of data that can be used by engineers to design possible solutions. At each tier of the DoD, goals and objectives, along with corresponding issues that may exist should

---

<sup>10</sup> Models, according to the DoDAF, are not prescriptive. The decision-makers and process owners will determine the DoDAF described models that are required for their purposes. For more information, and a list of the viewpoints, visit [http://dodcio.defense.gov/dodaf20/dodaf20\\_models.aspx](http://dodcio.defense.gov/dodaf20/dodaf20_models.aspx)

be addressed according to the established scope and purpose, (e.g., Departmental, Capability, SE, and Operational), as shown in the notional diagram in the figure below:

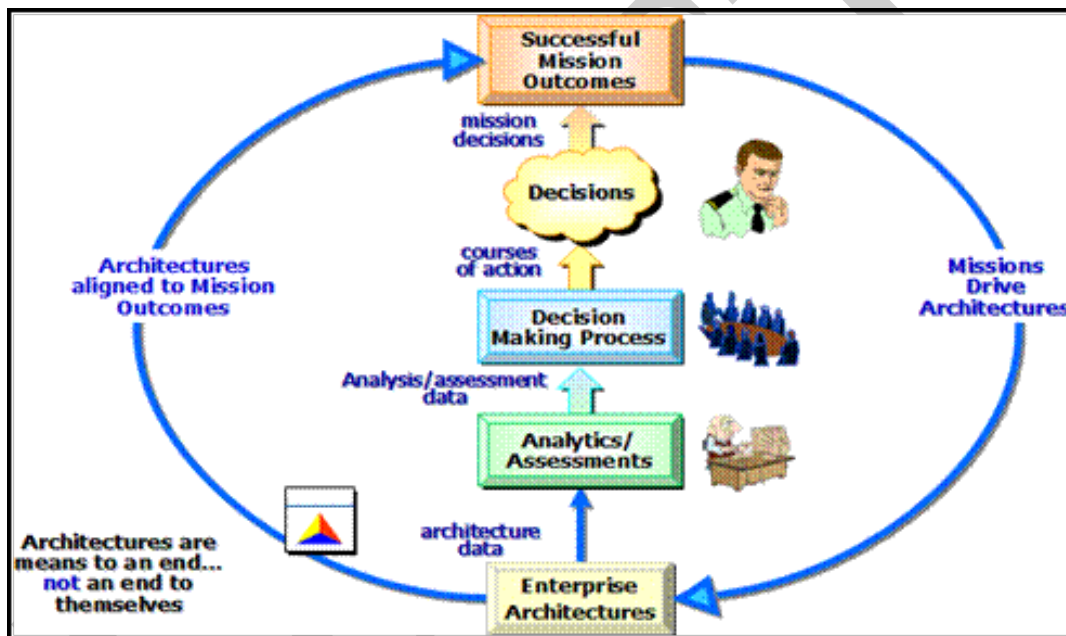


**Figure 4-1: Establishing the Scope for Architecture Development**

Establishing a scope for an architecture effort at any tier is similarly critical in determining the architecture boundaries, along with establishing the data categories needed for analysis and management decision-making. Scope also defines the key players whose input, advice, and consensus is needed to successfully architect and implement change (i.e., Stakeholders, both internal and external). Importantly, scope also determines the goals and objectives of the effort consistent with both boundaries and stakeholders, since goals and objectives define both the purpose for architecture creation and the level of architecture. Establishing the scope of an effort also determines the level of complexity for data collection and information presentation.

Architecture development also requires an understanding of external requirements that may influence architecture creation. An architecture developed for an internal agency purpose still needs to be mappable and consistent with higher level architectures and mappable to the DoD Enterprise Architecture (EA). For some architecture developments, consideration must be given in data collection and graphical presentation to satisfaction of other external requirements, such as upward reporting and submission of architectural data and models for program review, funding approval, or budget review due to the sensitivity or dollar value of the proposed solution.

Architecture scoping must facilitate alignment with, and support the decision-making process and ultimately mission outcomes and objectives as shown in the figure below. Architectural data and supporting views are created from organizing raw data into useful information, and collected into a useful viewpoint. The data should enable domain experts, program managers, and decision makers to utilize the architecture to locate, identify, and resolve definitions, properties, facts, constraints, inferences, and issues. This should apply within and across architectural boundaries that are redundant, conflicting, missing, and/or obsolete. DoDAF V2.0 provides the flexibility to develop both Fit-for-Purpose Views (User-developed Views and views from DoDAF-described Models) to maximize the capability for decision-making at all levels. The figure below shows how the development of architectures supports the management decision process. In this case, the example shows how an architecture, and the use of it in analysis, can facilitate the ability to determine and/or validate mission outcome.



**Figure 4-2: Mission Outcomes Supported by Architectures**

Analysis also uncovers the effect and impact of change (“what if”) when something is redefined, redeployed, deleted, moved, delayed, accelerated, or is no longer funded. Having a disciplined process for architecture development in support of analytics will produce quality results, not be prone to misinterpretations, and therefore, be of high value to decision makers and mission outcomes.

#### 4.2.3 Task: Determine a DoDAF Viewpoint and Model

DoDAF has been designed to meet the specific business and operational needs of the DoD. It defines a way of representing an enterprise architecture that enables stakeholders to focus on specific areas of interests in the enterprise, while retaining sight of the big picture. To assist decision-makers, DoDAF provides the means of abstracting essential

information from the underlying complexity and presenting it in a way that maintains coherence and consistency. One of the principal objectives is to present this information in a way that is understandable to the many stakeholder communities involved in developing, delivering, and sustaining capabilities in support of the stakeholder's mission. It does so by dividing the problem space into manageable pieces, according to the stakeholder's viewpoint, further defined as DoDAF-described Models.

Each viewpoint has a particular purpose and usually presents one or a combination of the following:

- Broad summary information about the whole enterprise (e.g., high-level operational concepts).
- Narrowly focused information for a specialist purpose (e.g., system interface definitions).

Information about how aspects of the enterprise are connected (e.g., how business or operational activities are supported by a system, or how program management brings together the different aspects of network enabled capability).

However, it should be emphasized that DoDAF is fundamentally about creating a coherent model of the enterprise to enable effective decision-making. The presentational aspects should not overemphasize the pictorial presentation at the expense of the underlying data.

DoDAF organizes the DoDAF-described Models into the following viewpoints:

- The **All Viewpoint** describes the overarching aspects of architecture context that relate to all viewpoints.
- The **Capability Viewpoint** articulates the capability requirements, the delivery timing, and the deployed capability.
- The **Data and Information Viewpoint** articulates the data relationships and alignment structures in the architecture content for the capability and operational requirements, system engineering processes, and systems and services.
- The **Operational Viewpoint** includes the operational scenarios, activities, and requirements that support capabilities.
- The **Project Viewpoint** describes the relationships between operational and capability requirements and the various projects being implemented. The Project Viewpoint also details dependencies among capability and operational requirements, system engineering processes, systems design, and services design within the Defense Acquisition System process. An example is the Vcharts in Chapter 4 of the Defense Acquisition Guide.
- The **Services Viewpoint** is the design for solutions articulating the Performers, Activities, Services, and their Exchanges, providing for or supporting operational and capability functions.



- The **Standards Viewpoint** articulates the applicable operational, business, technical, and industry policies, standards, guidance, constraints, and forecasts that apply to capability and operational requirements, system engineering processes, and systems and services.
- The **Systems Viewpoint**, for Legacy support, is the design for solutions articulating the systems, their composition, interconnectivity, and context providing for or supporting operational and capability functions.

A presentation of these viewpoints is portrayed in graphic format in the figure below.

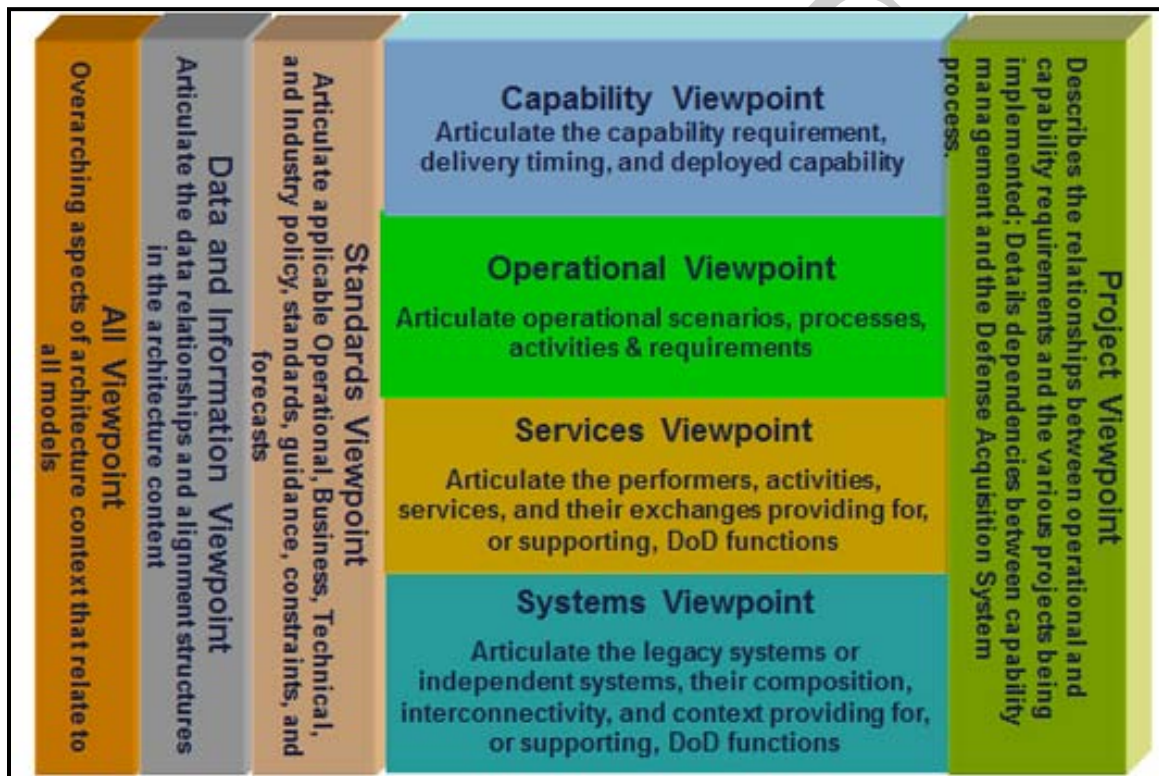


Figure 4-3: DoDAF Viewpoints and Models



## 5. WRITE SPECIFICATIONS & DOCUMENT DEVELOPMENT

**Qualification Standard:** Write detailed functional specifications that document the architecture development process.

### 5.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the Qualification Standard listed in this section:

[https://powhatan.iie.disa.mil/specialty\\_courses/](https://powhatan.iie.disa.mil/specialty_courses/).

### 5.2. Implementation<sup>11</sup>

Architects typically collect and organize data through the use of architecture techniques designed to use views (e.g., activity, process, organization, and data models as views) for presentation and decision-making purposes. The architectural data should be stored in a recognized commercial or government architecture tools.

#### 5.2.1 Task: Collect, Organize, Correlate, and Store Architectural Data

Designation of a data structure for the Architectural Description effort involves creation of a taxonomy to organize the collected data. This effort can be made considerably more simple by leveraging existing artifacts registered in the DoD Architecture Registry System (DARS), to include data taxonomies and data sets. Each Community of Interest (COI) maintains its registered data on DARS, either directly or through a federated approach. In addition, some organizations, such as U.S. Joint forces Command (JFCOM), have developed templates, which provide the basis of a customizable solution to common problems, or requirements, which includes datasets already described and registered in the DMR. Examples of this template-based approach are in the DoDAF Journal.

DARS provides more information that is specific, and guidance on retrieving needed data through a discovery process. Once registered data is discovered, the data can be cataloged and organized within a focused taxonomy, facilitating a means to determine what new data is required. New data is defined, registered in DARS, and incorporated into the taxonomy structure to create a complete defined list of required data. The data is arranged for upload to an automated repository to permit subsequent analysis and reuse. Discovery metadata (i.e., the metadata that identifies a specific Architectural Description, its data, views, and usage) should be registered in DARS as soon as it is available to support discovery and enable federation. Architects and data managers should use the DoD EA Business Reference Model (DoD EA BRM) taxonomy elements as the starting point for their registration efforts. Additional discovery metadata, such as processes and services may be required later, and should follow the same registration process.

---

<sup>11</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

### 5.2.2 Task: Document Results in Accordance with Decision-Maker Needs

The DoDAF architecture development process involves a step for the creation of architectural views based on queries of the underlying data. Presenting the architectural data to varied audiences requires transforming the architectural data into meaningful presentations for decision-makers. This is facilitated by the data requirements determined in the “Determine Data Required to Support Architecture Development” step, which is Step 3 of the 6-step DoDAF architecture development process. It is also facilitated by the data collection methods employed during Step 4 of the 6 step DoDAF architecture development process.

DoDAF V2.0 provides for models and views. DoDAF-described Models are those that enable a Systems Architect and development team whose data has already been defined and described consistent with the DM2. The models become views when they are populated with architectural data. These models include those previously described in earlier version of DoDAF, along with new models incorporated for the MODAF, the NATO NAF, and TOGAF that have relevance to DoD architecture development efforts.

Fit-for-Purpose Views are user-defined views that an architect and development team can create to provide information necessary for decision-making in a format customarily used in an agency. These views should be developed consistent with the DM2, but can be in formats (e.g., dashboard, charts, and graphical representations) that are normally used in an agency for briefing and decision purposes. An Architectural Description development effort can result in an Architectural Description that is a combination of DoDAF-described Models and Fit-for-Purpose Views.

DoDAF does not require specific models or views, but suggests that local organizational presentation types that can utilize DoDAF-created data are preferred for management presentation. A number of available architecture tools support the creation of views described in this step. The PES provides the format for data sharing.

**Note:** DoDAF V2.0 does NOT prescribe a Physical Data Model, leaving that task to the software developers who will implement the principles and practices of DoDAF in their own software offerings.

## 6. SPECIFY POWER SUPPLY REQUIREMENTS<sup>12</sup>

**Qualification Standard:** Specify power supply requirements and configuration based on system performance expectations and design specifications.<sup>13</sup>

### 6.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 6.2. Implementation

According to *DODI 8500.2, Subject Area Continuity, Control Number COPS-3*, Electrical systems are configured to allow continuous or uninterrupted power to key IT assets and all users accessing the key IT assets to perform mission or business-essential functions. This may include an uninterrupted power supply coupled with emergency generators or other alternate power source.

#### 6.2.1 Task: Require the Use of a Dedicated Circuit

A dedicated circuit is a circuit that runs from the breaker box to only certain outlets. In most offices, a circuit might have many jobs. Using too many devices on one circuit causes the power to sag, which might cause systems to crash. Dedicated circuits keep this from happening.

#### 6.2.2 Task: Require the Use of Surge Suppressors

An electrical surge, which is a sudden increase in the voltage on a circuit, can destroy an unprotected IS. Every device should plug into a surge suppressor.

#### 6.2.3 Task: Require the Install of a Backup Power Supply

Many server systems come with two power supplies. If either power supply fails, it can be replaced without turning off the system. However, if the power from the power company fails, a true backup system is needed. There are a number of small battery-based backup systems that will provide a few hours of protection. A gasoline or diesel backup system can be used if power is needed for several days.

---

<sup>12</sup> *CompTIA Network+ Certification All-in-One Exam Guide, 5th Edition (Exam N10-005)*

<sup>13</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

#### 6.2.4 Task: Require the Use of Redundant Components

Many components inside the system can be made redundant. It is common to find servers with redundant power supplies where a power supply can be removed without shutting down. You can buy Network Interface Cards (NIC) that work together in the same PC, providing redundancy if one fails. There are even NICs that are hot swappable in case of component failure. Placing hard drives on separate controllers, like drive duplexing, provides excellent redundancy.

DRAFT

## 7. EVALUATE INTERFACE BETWEEN HARDWARE AND SOFTWARE

**Qualification Standard:** Evaluate interface between hardware and software and operational and performance requirements of overall system.<sup>14</sup>

### 7.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iie.disa.mil/specialty\\_courses/](https://powhatan.iie.disa.mil/specialty_courses/).

### 7.2. Implementation<sup>15</sup>

Computer architecture encompasses all of the parts of a computer system that are necessary for it to function, including the operating system, memory chips, logic circuits, storage devices, input and output devices, security components, buses, and networking interfaces. The interrelationships and internal working of all of these parts can be quite complex, and making them work together in a secure fashion consists of complicated methods and mechanisms.

#### 7.2.1 Task: Implement Multiprocessing

Some computers have more than one CPU for increased performance. An operating system must be developed specifically to be able to work with more than one processor. If the computer system is configured to work in symmetric mode, the processors are handed work as needed in a load-balancing environment. When a process needs instructions to be executed, a scheduler determines which processor is ready for more work. If a processor is going to be dedicated to a specific task or application, all other software would run on a different processor. When a processor is dedicated, the system is working in asymmetric mode, which often means the computer has some time-sensitive application that necessitates its own processor.

#### 7.2.2 Task: Implement Process Management

Operating systems, software utilities, and applications are static lines of code that are initialized and put into memory. Applications work as individual processes, and the operating system also has several different processes carrying out various types of functionality. A process is the set of instructions that is running. A program is not considered a process until it is loaded into memory and activated by the operating system. When a process is created, the operating system assigns resources to it, such as a memory

---

<sup>14</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

<sup>15</sup> Harris, Shon *CISSP, All in One CISSP Exam Guide, 6<sup>th</sup> Edition*

segment, CPU time slot, access to system applications programming interfaces, and files to interact with. The collection of the instructions and the assigned resources is referred to as a process. In essence, the operating system gives a process all the tools it needs and then loads the process into memory.

The operating system has many of its own processes, which are used to provide and maintain the environment for applications and users to work within. Operating systems provide multiprogramming, which means that more than one program or process can be loaded into memory at the same time.

### 7.2.3 Task: Implement Preemptive Multitasking

With preemptive multitasking, the operating system controls how long a process can be a resource. Through the use of time sharing, the system can suspend a process that is using the CPU and allow another process access to it. By using preemptive multitasking, one application does not negatively affect another application as easily as when using cooperative multitasking.

### 7.2.4 Task: Determine Whether to Run Processes in a Running State, Ready State, or Blocked State

A process can be in a running state, which is when the CPU is executing its instructions and data; a ready state, which is when it's waiting to send instructions to the CPU; or a blocked state, which is when it's waiting for input data from a user.

### 7.2.5 Task: Utilize Thread Management

A thread is made up of an individual instruction set and the data that must be worked on by the CPU. Most applications have several different functions. Each one of these functions requires a thread to be dynamically generated, and threads are dynamically created and destroyed as needed. Some applications are multi-threaded and can run several different threads simultaneously. Software security ultimately comes down to whether threads and processes are behaving properly. If a thread misbehaves and it is working in a privileged mode, then it can carry out malicious activities that affect critical resources of the system. Attackers can inject code into a running process to carry out some type of compromise. Software developers need to make sure that running processes will not accept unqualified instructions and allow for these types of compromises. Processes should only accept instructions for an approved entity and the instruction that it accepts should be validated before execution.

### 7.2.6 Task: Enforce Process Isolation

Operating systems commonly have functionality that implements process isolation to protect processes from each other. Process isolation is necessary to ensure that processes do not communicate in an insecure manner or negatively affect each other's productivity. With process isolation, if one process hangs for some reason, it will not affect the other software running. The following methods can be used to enforce process isolation:

- Encapsulation of objects

- Time multiplexing of shared resources
- Naming distinctions
- Virtual memory mapping

#### 7.2.7 Task: Implement Memory Management

To provide a safe and stable environment, an operating system must exercise memory management. The goals of memory management are to:

- Provide an abstraction level for programmers
- Maximize performance with the limited amount of memory available
- Protect the operating system and applications loaded into memory

#### 7.2.8 Task: Avoid Buffer Overflow

When a programmer writes a piece of software that will accept data, this data and its associated instructions will be stored in the buffers that make up a stack. The buffers need to be the right size to accept the inputted data. If a programmer does not ensure that only one byte of data is being inserted into the software, then a hacker can input several characters at once and overflow that specific buffer.

#### 7.2.9 Task: Avoid Memory Leaks

When an application makes a request for a memory segment to work within, it is allocated a specific memory amount by the operating system. When the application is done with the memory, it is supposed to tell the operating system to release the memory, which makes it available to other applications. Some applications are written poorly and do not indicate to the system that the memory is no longer in use. If this happens enough times, the operating system could become starved for memory, which would negatively impact the system's performance. When a hacker identifies a memory leak, the door is opened to new denial-of-service (DoS) attacks.

#### 7.2.10 Task: Implement Input/Output Device Management

An operating system also has to control all input/output devices. It sends commands to them, accepts their interrupts when they need to communicate with the CPU, and provides an interface between the devices and the applications. The operating system uses a device driver to communicate with a device controller. Operating systems also need to access and release devices and computer resources properly. Different operating systems handle accessing devices and resources differently. Later versions of Windows have a very controlled method of accessing devices. This method helps protect the system from badly written code that does not properly request and release resources. Such a level of protection helps ensure the resources' integrity and availability.

## 8. DOCUMENT DESIGN SPECIFICATIONS

**Qualification Standard:** Document design specifications, installation instructions, and other system-related information.<sup>16</sup>

### 8.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 8.2. Implementation<sup>17</sup>

The *Systems Engineering Plan (SEP) Outline*, produced by the Office of the Deputy Assistant Secretary of Defense (ODASD), serves as a mandated format for all systems engineering plans. The following tasks outline the procedures Systems Architects/Engineers should follow when documenting design specifications, installation instructions, and other system-related information.

#### 8.2.1 Task: List the Architecture Products That Will be Developed

List the architecture products that will be developed, to include system level physical and software architectures and DODAF architectures. Summarize the approach for architecture development to include:

- Program's DODAF architecture development efforts.
- A system physical architecture diagram (delineating physical interfaces), if available.
- A system functional architecture diagram (delineating functional interfaces), if available.
- How software architecture priorities will be developed and documented.
- How architecture products are related to requirements definition.
- How engineering and architecture activities are linked.

---

<sup>16</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

<sup>17</sup> OPR: ADASD (Systems Engineering), *Systems Engineering Plan (SEP) Outline, Version 1.0*, 20 April 2011



## 8.2.2 Task: Summarize the System-Level Technical Certifications Obtained

Use the following table to summarize the system-level technical certification which must be obtained during a program's lifecycle.

Table 8-1: Technical Certifications<sup>18</sup>

Certification	PMO Team/PoC	Activities to Obtain Certification <sup>1</sup>	Certification Authority	Expected Certification Date
Airworthiness	Airframe IPT			?Q FY?
Clinger Cohen		Confirm compliance	Component CIO (MDAP/MAIS also by DoD CIO)	?Q FY?
Transportability				?Q FY?
Insensitive Munitions	Manufacturing WG	Reference Document: <i>PEO IM Strategic Plan</i>		?Q FY?
Etc.				?Q FY?

## 8.2.3 Task: Create a Technical Schedule and Schedule Risk Analysis

When creating a technical schedule and scheduling a risk assessment, the following questions should be answered:

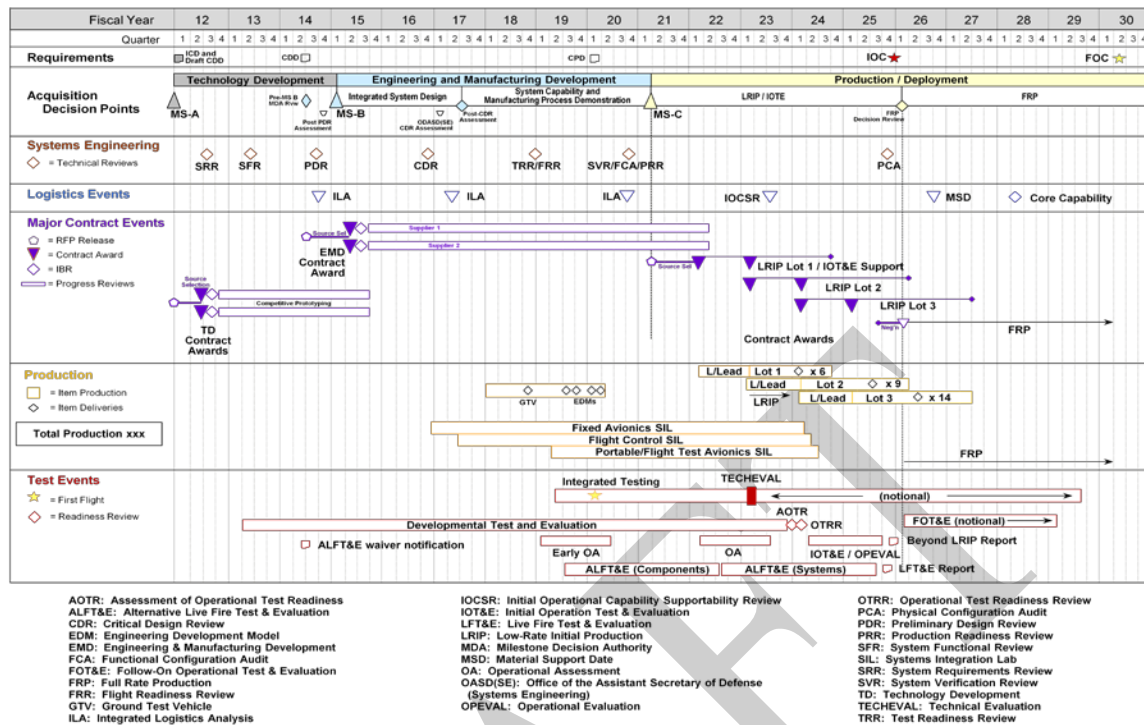
- Who is responsible for technical schedule planning and execution?
- How are program tasks identified and managed?

The Systems Architect should also list scheduling and/or planning assumptions, and identify which program office position or team is responsible for keeping the schedule up-to-date. A sample schedule follows:

<sup>18</sup> OPR: ADASD (Systems Engineering), *Systems Engineering Plan (SEP) Outline*

# UNCLASSIFIED//FOR OFFICIAL USE ONLY

## SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1



**Figure 8-1: Detailed Technical Schedule<sup>19</sup>**

The Systems Architect should also provide a detailed, integrated, lifecycle system schedule to include:

Planned milestones and planned significant activities (viz., activities which must be performed in order to produce the system):

- Systems Engineer (SE) technical reviews
- Technology on/off –ramps
- RFP release dates
- Software releases
- Hardware (HW)/Software (SW) Integration events
- Key developmental, operational, integrated testing
- Technology Readiness Assessments (TRAs)
- Contract award (including bridge contracts)
- Testing events/phases
- System-level certifications

<sup>19</sup> OPR: ADASD (Systems Engineering), *Systems Engineering Plan (SEP) Outline*

The Systems Architect should schedule a Risk Assessment.

Summarize the program's schedule risk assessment (SRA) process and its results to include:

- What SRA techniques will be used to determine program schedule risk (e.g., critical path analysis, Monte Carlo simulations, etc.).
- Inherent impact of schedule constraints and dependencies and actions taken or planned to mitigate schedule drivers.
- Results of any SRAs accomplished.
- List significant critical path or likely critical path events/activities and any planned actions to reduce risk for each.

#### 8.2.4 Task: List and Summarize the Program Oversight and Management Systems

List and summarize the program oversight and management systems that will integrate cost, schedule, and technical performance goals, metrics, and resources. Specifically address:

- Work Breakdown Structure (WBS)
  - Summarize the relationship among the WBS, product structure, and schedule.
  - Identify the stakeholders who will develop the WBS.
  - Explain the traceability between the system's technical requirements and WBS.
- Integrated Master Plan (IMP)/ Integrated Master Schedule (IMS)
  - What is the relationship of the program's IMP to the contractor(s) IMS; how are they linked/interfaced; and what are their primary data elements?
  - Who or what team is responsible for developing the IMP; when is it required; will it be a part of the Request for Proposal (RFP)?
  - If used, how will the program use earned value management (EVM) cost reporting to track/monitor the status of IMS execution?

#### 8.2.5 Task: Diagram the Process for How the Program Plans to Manage Engineering

Diagram the process for how the program plans to manage engineering and integration risk and how these processes will be integrated with the contractor(s). This should include how the Project Management Office (PMO) will identify and analyze risks; and plan for, implement (including funding), and track risk mitigation.

**8.2.6 Task: Indicate Roles, Responsibilities, and Authorities Within the Risk Management Process**

Indicate roles, responsibilities, and authorities within the risk management process for:

- Reporting/identifying risks
- Criteria used to determine if a “risk” submitted for consideration will become a risk or not (typically, criteria for probability and consequence)
- Adding/modifying risks
- Changing likelihood and consequence of a risk
- Closing/retiring a risk

If Risk Review Boards or Risk Management Boards are part of the process, indicate who are the chair and participants and how often they meet.

List the risk tool(s) the program (program office and contractor(s)) will use to perform risk management.

If program office and contractor(s) use different risk tools, how will the information be transferred across them? NOTE: In general, the same tool should be used. If the contractor’s tool is acceptable, then this merely requires Government direct, networked access to that tool.

**8.2.7 Task: Provide a Listing of the Current System-Level Technical Risks**

**Technical Risks and Mitigation Planning** – Provide a risk cube or a listing of the current system-level technical risks with:

- As-of date
- Risk rating
- Description
- Driver
- Mitigation status

**8.2.8 Task: Provide Planned Program Office Organization Structure**

Provide planned program office organization structure (i.e., wiring diagram to illustrate hierarchy) with an as-of date and include the following elements:

- Legend, as applicable (e.g., color-coding)
- Organization to which the program office reports
- Functional Leads (e.g., T&E, logistics, risk, reliability, software)
- Program Manager (PM)
- Lead/Chief Systems Engineer

- Core, matrix, and contractor support
- Field or additional Service representatives

#### 8.2.9 Task: Summarize the Program's Technical Staffing Plan

Summarize the program's technical staffing plan to include:

- Process and tools program will use to determine required technical staffing;
- Risks and increased demands on existing resources if staffing requirements are not met;
- A figure (e.g., sand chart) to show the number of required full-time equivalent (FTE) positions (e.g., organic, matrix support, and contractor) by key program events (e.g., milestones and technical reviews).

#### 8.2.10 Task: Describe Relationships with External Technical Organizations

Describe what processes or methods will be used to document, facilitate, and manage interaction among SE team(s), external-to-program government organizations (e.g., Family of Systems (FoS)/Systems of Systems (SoS) and contractor(s)/ competing contractor(s)) on technical tasks, activities, and responsibilities (e.g., requirements, technical baselines, and technical reviews) down to and including subcontractors.

**Responsible Organization and Authority** - Identify the organization responsible for coordinating SE and integration efforts associated with the FoS/SoS and its authority to reallocate resources (funding and manpower).

**Management** – Summarize how FoS/SoS interfaces will be managed to include:

- Resolution of issues that cross PM, PEO, and Component lines;
- Interface Control Documents (ICDs) and any interface control Working Groups (ICWGs);
- Memorandums-of-Agreement (MOAs);
- “Triggers” that require a FoS/SoS member to inform the others if there is a cost, schedule, or performance deviation;
- Planned linkage between hardware and software upgrade programs within the FoS/SoS;
- Any required Government Furnished Equipment/Property/Government Furnished Information (GFE/GFP/GFI) (e.g., test ranges, integration laboratories, and special equipment).

**Schedule** - Include a schedule (optional) which shows FoS/SoS dependencies such as alignment of technical reviews, major milestones, test phases, GFE/GFP/GFI, etc.

#### 8.2.11 Task: Identify Technical Performance Measures and Metrics

What is the program's strategy for identifying, prioritizing, and selecting the set of metrics for monitoring and tracking program SE activities and performance? This explanation should include:

- An overview of the measurement planning and metrics selection process, including the approach to monitor execution to the established plan, and identification of roles, responsibilities, and authorities for this process.
- A minimum set of technical performance measures (TPMs) and intermediate goals and the plan to achieve them with as-of dates (to provide quantitative insight into requirements stability and specification compliance). Examples include TPMs in the areas of software, reliability, manufacturing, and integration to assess "execution to plan."
- For reliability, PMs shall use a growth curve to plan, illustrate, and report progress. Growth curves will be stated in a series of intermediate goals and tracked through fully integrated, system-level test and evaluation events until the reliability threshold is achieved. If a single curve is not adequate to describe overall system reliability, provide curves for critical subsystems with rationale for their selection.

#### 8.2.12 Task: Summarize Technical Activities and Products

**Results of Previous Phase SE Activities** - Summarize (consider a tabular format) system-level technical reviews, trade studies, and independent reviews conducted to date; date(s) conducted; and key results or impact(s) to design and any related recommendations and status of actions taken. For Major Defense Acquisition Programs (MDAP), these reviews shall include an assessment of manufacturing risk and readiness.

**Planned SE Activities for the Next Phase** – Summarize key planned system engineering, integration, and verification processes and activities established or modified since the previous acquisition phase, including updated risk reduction and mitigation strategies and technical and manufacturing maturity.

**Analysis and Decomposition** – How will top-level requirements (i.e., from Analysis of Alternatives (AoA), Key Performance Parameters (KPP), Key System Attributes (KSA), statutory, regulatory, certification, safety, software, hardware, etc.) be traced from the source Joint Capabilities Integration and Development System (JCIDS) documents down to configuration item (CI) build-to specifications and Verification and Validation (V&V) plans?

- Identify which program office position or team (e.g., IPT/WG) is responsible for continuously ensuring the accurate traceability of requirements.
- Identify the tool (s) the program plans to use (or continues to use) for requirements traceability in Tools Table 4.7-1.
- If the program office and prime contractor(s) use different tools, how will information be transferred across them?

- What approach will be used to ensure that there are no orphan or childless requirements?
- Describe how the JCIDS sustainment characteristics were translated into Reliability & Manageability (R&M) contract specifications.

#### 8.2.13 Task: Document Requirements Management and Change Process

**Requirements Management and Change Process** – How will requirements be managed and changes made and tracked?

- If the program is a MDAP, and if it were to have a change in requirement which could result in a cost and/or schedule breach, summarize the mechanism by which the program will involve its Configuration Steering Board.
- Identify which program office position or team (e.g., IPT/WG) will be responsible for continuously ensuring the accurate management of requirements and requirement changes.

#### 8.2.14 Task: Summarize Plans for Conducting Technical Review

Refer to section 16 of this document.

#### 8.2.15 Task: Identify Engineering Tools the Program Plans to Use

In a table, similar to the sample below, identify the tools the program plans to use.

**Table 8-2: Sample Engineering Tools<sup>20</sup>**

Engineering Tool	Purpose	Position/IPT Responsibility
IMS		
IBM®Rational® DOORS®	Requirements Traceability and Verification Methodology and Completion	SE IPT/Rqmts Manager
Requirements Verification Matrix (RVM)	Requirements Verification	
Computer-Aided Three- Dimensional Interactive Application (CATIA)	Design	SE IPT

<sup>20</sup> OPR: ADASD (Systems Engineering), *Systems Engineering Plan (SEP) Outline*

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Risk Mgmt Information System (RMIS)	RM	SE IPT/Risk Manager
SW Integration Lab (SIL)	M&S	SW WG
SW Engineering	Design	SW WG
SW cost estimating (e.g., COCOMO)		SW WG
Producibility/Throughput Analysis Tool		Manufacturing WG
Line of Balance	Production planning	Manufacturing WG
Reliability Growth (e.g., RGA®, PM2, RGTm, AMPM)	Reliability growth planning and tracking	SE IPT/R&M Lead
Etc.		



## 9. ENSURE COMPATIBILITY OF SYSTEM COMPONENTS

**Qualification Standard:** Collaborate with system developers to select appropriate design solutions or ensure the compatibility of system components.<sup>21</sup>

### 9.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 9.2. Implementation<sup>22</sup>

A Systems Architect should ensure that all of the components of the system are compatible by having an in-depth understanding of the various components, then selecting appropriate design solutions accordingly.

#### 9.2.1 Task: Understand CPU Architecture

An operating system and a CPU must be able to communicate through an instruction set, which is a language an operating system must be able to speak to properly communicate to a CPU. The micro architecture contains the things that make up the physical CPU. The CPU knows mechanically how to use all of these parts, but it still needs to know what the operating system wants it to do. The CPU has a menu of operations the operating system can get an instruction set from. The operating system puts in its instruction set (render graphics on screen, print to printer, encrypt data, etc.), and the CPU carries out the request and provides the result.

The operating system and CPU have to work within the same ring architecture. In order to be stable, it must be able to protect itself from its users and their applications. This requires the capability to distinguish between operations performed on behalf of the operating system itself and operations performed on behalf of the users or applications.

The operating system has several protection mechanisms to ensure processes do not negatively affect each other or the critical components of the system itself. One discussed in a previous section is memory protection. Another is a ring-based architecture.

The CPU provides the ring structure architecture and the operating system assigns its processes to the different rings. When a process is placed in ring 0, its activities are carried out in kernel mode, which means it can access the most critical resources in a nonrestrictive manner.

---

<sup>21</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

<sup>22</sup> Harris, Shon *CISSP, All in One Exam Guide, 6<sup>th</sup> Edition*

Attackers have found ways around this protection scheme and have tricked operating systems into loading their malicious code into ring 0. Attackers have fooled operating systems by creating their malicious code to mimic system-based dynamic-link libraries (DLL), loadable kernel modules, or other critical files. The malicious code can install key loggers, sniffers, code injection tools, and Trojaned files. The code could delete files on the hard drive, install backdoors, or send sensitive data to the attacker's computer using the compromised system's network protocol stack.

### 9.2.2 Task: Understand Operating System Architecture

Operating system architectures deal specifically with the software components of a system. The architecture is the framework that dictates how the parts of the operating system interact with each other and provide the functionality that the applications and users require of it.

There are different types of operating system architectures described below:

- **Monolithic** – All operating system processes run in kernel mode.
- **Layered** – All operating system processes run in a hierarchical model in kernel mode.
- **Microkernel** – Core operating system processes run in kernel mode and the remaining ones run in user mode.
- **Hybrid microkernel** – All operating system processes run in kernel mode. Core processes run within a microkernel and others run in a client/server model.

### 9.2.3 Task: Apply Security Policy

Security starts at a policy level, which are high-level directives that provide the foundational goals for a system overall and the components that make it up from a security perspective. A security policy is a strategic tool that dictates how sensitive information and resources are to be managed and protected. A security policy expresses exactly what the security level should be by setting the goals of what the security mechanisms are supposed to accomplish. This is an important element that has a major role in defining the architecture and design of the system. The security policy is a foundation for the specifications of a system and provides the baseline for evaluating a system after it is built. The evaluation is carried out to make sure that the goals that were laid out in the security policy were implemented.

### 9.2.4 Task: Know How the Trusted Computing Base Works

The trusted computing base (TCB) is a collection of all the hardware, software, and firmware components within a system that provide some type of security and enforce the system's security policy.

The operating system's kernel is made up of hardware, software, and firmware. However, the TCB can include other components, such as trusted commands, programs, and configuration files that can directly interact with the kernel.

Every operating system has specific components that would cause the system grave danger if they were compromised. The components that make up the TCB provide extra layers of protection around these mechanisms to help ensure they are not compromised. The following are TCB components that must be developed securely:

- The BIOS function should have a password protection capability and be tamperproof.
- The subsystem within a Windows operating system that generates access tokens should not be able to be hijacked and be used to produce fake tokens for malicious processes.
- Before a process can interact with a system configuration file, it must be authenticated by the security kernel.
- Device drivers should not be able to be modified in an unauthorized manner.

#### 9.2.5 Task: Secure the Security Kernel

The security kernel is made up of hardware, software, and firmware components that fall within the TCB, and it implements and enforces the reference monitor concept.<sup>23</sup> The security kernel mediates all access and functions between subjects and objects. It is the core of the TCB and is the most commonly used approach to building trusted computing systems. The security kernel has three main requirements:

- 1) Provide isolation for the processes carrying out the reference monitor concept, and the processes must be tamperproof.
- 2) Must be invoked for every access attempt and must be impossible to circumvent.
- 3) Must be small enough to be tested and verified in a comprehensive manner.

---

<sup>23</sup> The reference monitor is an abstract machine that mediates all access subjects have to objects, both to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification.

## 10. EVALUATE CURRENT OR EMERGING TECHNOLOGIES

**Qualification Standard:** Evaluate current or emerging technologies to consider factors such as cost, security, compatibility, or usability.<sup>24</sup>

### 10.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 10.2. Implementation

The Defense Acquisition Guide should be used by the Systems Architect to evaluate current or emerging technologies. The information described below can be found at <https://acc.dau.mil/CommunityBrowser.aspx?id=638297>.

#### 10.2.1 Task: Use the Defense Acquisition Guide (DAG)

The practice of systems engineering (SE) is composed of 16 processes: eight technical processes and eight technical management processes as described in *DAG section 4.3 Systems Engineering Processes*. These 16 processes provide a structured approach to increasing the technical maturity of a system and increasing the likelihood that the capability being developed balances mission performance with cost, schedule, risk, and design constraints.

The eight technical management processes are implemented across the acquisition life cycle and provide insight and control to assist the Program Manager and Systems Engineer to meet performance, schedule, and cost goals. The eight technical processes closely align with the acquisition life-cycle phases and include the top-down design processes and bottom-up realization processes that support transformation of operational needs into operational capabilities.

The ultimate purpose of the SE processes is to provide a framework that allows the SE team to efficiently and effectively deliver a capability to satisfy a validated operational need. To fulfill that purpose, a program implements the SE technical processes in an integrated and overlapping manner to support the iterative maturation of the system solution. The level of SE required supporting these processes declines as a program progresses into the later phases of the acquisition life cycle. Implementation of the SE processes begins with the identification of a validated operational need as shown in the top left corner of the V-diagram. The technical processes enable the SE team to ensure that the delivered capability accurately reflects the operational needs of the stakeholders.

---

<sup>24</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

The key activities that are accomplished by the execution of the technical processes are described below:

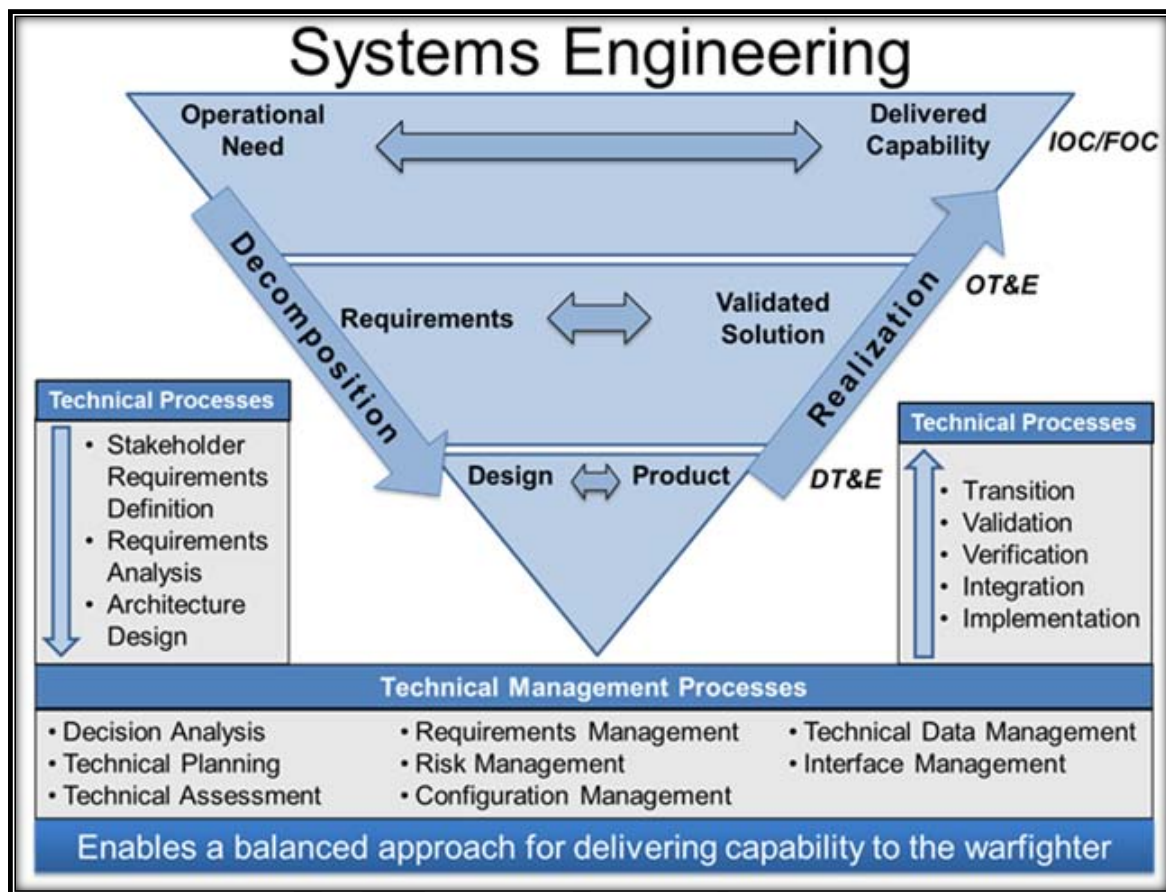
During the Stakeholder Requirements Definition process, the operational requirements and inputs from relevant stakeholders are translated into a set of top level technical requirements. These requirements are decomposed and elaborated during the Requirements Analysis process to produce a complete set of system functional and performance requirements.

During the Architecture Design process, the Systems Engineer, often through system modeling, trade-offs, and decision analyses, captures the functional requirements and interdependencies in the system architecture. Trade-offs and analyses are also used to mature and realize the design of the system and system elements during the Implementation process, generating the product baseline.

During the Integration process, the program assembles the system elements together to provide the system for testing in the Verification process (developmental tests verifying the functional requirements) and Validation process (operational tests validating the system meets the operational need), resulting in a validated solution.

During the Transition process, the program formally delivers the system capability to the end users, including all enabling system elements to support operational use and sustainment activities.

The technical management processes shown in the figure below provide a consistent approach to managing the program's technical activities and controlling information and events that are critical to the success of the program. Taken together, these 16 processes are a systematic approach focused on providing operational capability to the warfighter while reducing technical and programmatic risk.



**Figure 10-1: Technical Management Processes**

All organizations performing SE should scale their application and use of the processes in DAG section 4.3. Systems Engineering Processes to reflect the unique needs of the program and the type of product or system being developed. This scaling should reflect the system's maturity and complexity, size and scope, life-cycle phase, and other relevant considerations. For example, lower-risk, less-complex programs may scale the processes to ensure key activities are effective but not overly cumbersome (e.g., simpler and less-expensive tools, less-frequent reporting, and activities adjusted to fit smaller organizations with fewer personnel).

The Systems Engineer contributes to defining, establishing, and achieving affordability targets throughout the life cycle of the system. Affordability targets are based on what the Department can afford to spend for the capability, including program acquisition and sustainment costs. Affordability targets are used as design constraints in the development, procurement, and sustainment of an affordable system. See DAG section 4.3.18.2.

Affordability – Systems Engineering Trade-Off Analyses, for more information on how affordability drives design decisions.

The Program Manager controls requirements growth and should use affordability goals early in the process to guide design trades and program decisions. The Systems Engineer

assists in managing affordability by working closely with the program cost estimator/analyst team when developing common cost and technical models and aligning baselines. See [DAG Chapter 3 Affordability and Life-Cycle Resource Estimates](#) for more information on affordability.

Throughout the acquisition life cycle, the Program Manager and Systems Engineer should monitor the system affordability, seek out cost saving opportunities, and identify any associated cost, schedule, and performance risks. The Program Manager's emphasis prior to Milestone B should be on defining and achieving affordability targets and desired capabilities. During the Technology Development (TD) phase, the Program Manager and Systems Engineer work to reduce technical risk and develop a sufficient understanding of the materiel solution development to validate design approaches and cost estimates, to refine requirements and to ensure affordability is designed in to the desired capability. After Milestone B, the emphasis shifts to defining and achieving should cost estimates.

Should cost management is a deliberate strategy to drive cost efficiencies and productivity growth into programs. The will cost estimate is the likely life-cycle cost of the system based on historical data and represents the program's independent cost estimate, i.e., as generated by the Cost Assessment and Program Evaluation (CAPE) office or Service equivalent. As the program identifies inefficiencies, the Should Cost estimate is developed based on specific actions and opportunities to mitigate, eliminate, or reduce those inefficiencies that allow the program to come in below the expected will cost estimates. The Program Manager, with support from the Systems Engineer, develops program office cost estimates reflecting should cost opportunities and plans. The Program Manager uses the cost estimate as a tool to:

- 1) Influence design trades and choices when analyzing and setting contract/production execution targets
- 2) Manage all costs throughout the product's life cycle
- 3) Manage the product's final unit and sustainment cost
- 4) Provide incentives for both of the parties (Government and industry) to execute efficiently: Government managers, who seek more value for the warfighter and taxpayer; and industry managers, who develop, build and sustain the systems and provide needed services

Should cost focuses on controlling the cost of both current and planned work. To have an impact, these activities should inform contract negotiations leading up to Engineering and Manufacturing Development (EMD) and Production and Deployment (P&D) phases.

Should cost management does not mean trading away the long-term value of sound design practices and disciplined SE activities for short-term gain; it does mean eliminating non-value-added activities and reports that are not required and that are deemed unessential. For guidance on implementing should cost management, see the [Better Buying Power website](#).

Program Managers address affordability requirements and begin to apply should cost management early in the acquisition life cycle. This includes applying SE to define an

affordable system design while also working to eliminate inefficiencies and duplication where applicable and to drive productivity improvements into their programs.

DRAFT



## 11. DEVELOP A SYSTEM SECURITY CONTEXT

**Qualification Standard:** Develop a system security context, a preliminary system security CONOPS, and define baseline system security requirements in accordance with applicable IA requirements.<sup>25</sup>

### 11.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 11.2. Implementation

An important concept in the design and analysis of secure systems is the security model, because it incorporates the security policy that should be enforced in the system. A model is a symbolic representation of a policy.

#### 11.2.1 Task: Implement a Security Model

A security model maps the abstract goals of the policy to information system terms by specifying explicit data structures and techniques necessary to enforce the security policy. A security model is usually represented in mathematics and analytical ideas, which are mapped to system specifications and then developed by programmers through programming code.

The following are core concepts of different viable security models:

**Bell-LaPadula model** – It was the first mathematical model of a multilevel security policy that defines the concept of a secure state and necessary modes of access. It ensures that information only flows in a manner that does not violate the system policy and is confidentiality focused.

- The simple security rule – A subject cannot read data at a higher security level
- The \*-property rule – A subject cannot write to an object at a lower security level
- The strong star property rule – A subject can perform read and write functions only to the objects at its same security level

**Biba model** – A formal state transition model that describes a set of access control rules designed to ensure data integrity.

- The simple integrity axiom – A subject cannot read data at a lower integrity level

---

<sup>25</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

- The \*-integrity axiom – A subject cannot modify an object in a higher integrity level

**Clark-Wilson model** – This integrity model is implemented to protect the integrity of data and to ensure that properly formatted transactions take place. It addresses all three goals of integrity:

- Subjects can access objects only through authorized programs
- Separation of duties is enforced
- Auditing is required

**Information flow model** – This is a model in which information is restricted in its flow to only go to and from entities in a way that does not negate or violate the security policy.

**Noninterference model** – This formal multilevel security model states that commands and activities performed at one security level should not be seen by, or affect, subjects or objects at a different security level.

**Brewer and Nash model** – This model allows for dynamically changing access controls that protect against conflicts of interest. Also known as the Chinese Wall model.

**Graham-Denning model** – This model shows how subjects and objects should be created and deleted. It also addresses how to assign specific access rights.

**Harrison-Ruzzo-Ullman model** – This model shows how a finite set of procedures can be available to edit the access rights of a subject.

#### 11.2.2 Task: Conduct an Assurance Evaluation

An assurance evaluation examines the security-relevant parts of a system, meaning the TCB, access control mechanisms, reference monitor, kernel, and protection mechanisms. The relationship and interaction between these components are also evaluated. There are different methods of evaluating and assigning assurance levels to a system. For more information regarding how the DoD assigns assurance levels to a system, refer to section 14 of this guide.

#### 11.2.3 Task: Implement Security Modes of Operation Used in Mission Assurance Category (MAC) Systems

A multilevel security system can operate in different modes depending on the sensitivity of the data being processed, the clearance level of the users, and what those users are authorized to do. The mode of operation describes the security conditions under which the system functions. The modes that are discussed in this section are used in MAC systems, which hold one or more classifications of data. The following things should be considered when determining the mode the operating system should be working in:

- The types of users who will be connecting to the system
- The type of data processed on the system

- The clearance levels, need-to-know, and formal access approvals the users will have

The following describes the different security modes that multilevel operating systems can be developed and configured to work in:

### **Dedicated Security Mode**

All users must have...

- Proper clearance for all information on the system
- Formal access approval for all information on the system
- A signed Non-Disclosure Agreement (NDA) for all information on the system
- A valid need-to-know for all information on the system
- All users can access all data

### **System High-Security Mode**

All users must have...

- Proper clearance for all information on the system
- Formal access approval for all information on the system
- A signed NDA for all information on the system
- A valid need-to-know for all information on the system
- All users can access some data, based on their need-to-know

### **Compartmented Security Mode**

All users must have...

- Proper clearance for the highest level of data classification on the system
- Formal access approval for some information on the system
- A signed NDA for all information they will access on the system
- A valid need-to-know for some of the information on the system
- All users can access some data, based on their need-to-know and formal access approval

### **Multilevel Security Mode**

All users must have...

- Proper clearance for some of the information on the system
- Formal access approval for some of the information on the system
- A signed NDA for all information on the system

- A valid need-to-know for some of the information on the system
- All users can access some data, based on their need-to-know, clearance, and formal access approval

#### 11.2.4 Task: Understand the Common Criteria (CC)

The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that:

- 1) Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfillment of particular security properties, to a certain extent or assurance;
- 2) Supporting documents, are used within the Common Criteria certification process to defines how the criteria and evaluation methods are applied when certifying specific technologies;
- 3) The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;
- 4) These certificates are recognized by all the signatories of the CCRA.

The CC is the driving force for the widest available mutual recognition of secure IT products. To obtain information on specific security functional requirements and security assurance requirements, visit <http://www.commoncriteriaportal.org/cc/>.

## 12. ADDRESS DOD ENGINEERING REQUIREMENTS

**Qualification Standard:** Document and address DoD IS, IA architecture, and systems security engineering requirements throughout the acquisition life-cycle.<sup>26</sup>

### 12.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 12.2. Implementation

For the sake of this procedure guide, the roles of Systems Architect and Systems Engineer are interchangeable. The Defense Acquisition Guidebook (DAG), Chapter 4, provides overarching guidance on the systems engineering (SE) discipline, its activities and processes, and its practice in defense acquisition programs. The Program Manager and the Systems Engineer should use DAG and the Defense Acquisition Management System to effectively plan and execute program activities across the system life cycle.

#### 12.2.1 Task: Utilize the Defense Acquisition Management System

Evolutionary acquisition is the preferred DoD strategy for rapid acquisition of mature technology for the user. An evolutionary approach delivers capability in increments, recognizing up front the need for future capability improvements. The objective is to balance needs and available capability with resources, and to put capability into the hands of the user quickly. The success of the strategy depends on phased definition of capability needs and system requirements, and the maturation of technologies that lead to disciplined development and production of systems that provide increasing capability over time.

Evolutionary acquisition requires collaboration among the user, tester, and developer. In this process, a needed operational capability is met over time by developing several increments, each dependent on available mature technology. Technology development preceding initiation of an increment shall continue until the required level of maturity is achieved, and prototypes of the system or key system elements are produced. Successive Technology Development Phases may be necessary to mature technology for multiple development increments.

Each increment is a militarily useful and supportable operational capability that can be developed, produced, deployed, and sustained. Each increment will have its own set of threshold and objective values set by the user. Block upgrades, pre-planned product improvement, and similar efforts that provide a significant increase in operational

---

<sup>26</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

capability and meet an acquisition category threshold specified in this document shall be managed as separate increments under this Instruction.

For more specific information on how to use the Defense Acquisition Management System, refer to [the Defense Acquisition Management System](#) online by clicking this link.

#### 12.2.2 Task: Utilize the Defense Acquisition Guidebook (DAG)

*DAG for Systems Engineering Chapter 4* provides overarching guidance on the systems engineering (SE) discipline, its activities and processes, and its practice in defense acquisition programs. The Program Manager and the Systems Engineer should use *DAG Chapter 4* to effectively plan and execute program activities across the system life cycle.

Refer to Section 10 of this Guide, *Evaluate Current or Emerging Technologies to Consider Factors Such as Cost, Security, Compatibility, or Usability*, to better understand guidance for the Systems Engineer in the Defense Acquisition Guidebook. For specific instructions on how to apply this guidance, please visit the [Defense Acquisition Guidebook](#) online by clicking this link.

## 13. IDENTIFY PROTECTION NEEDS

**Qualification Standard:** Identify protection needs for information systems and networks and document appropriately.<sup>27</sup>

### 13.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iie.disa.mil/specialty\\_courses/](https://powhatan.iie.disa.mil/specialty_courses/).

### 13.2. Implementation

Security design is one of the most important aspects of system design. An overall goal that most organizations have is that security problems not disrupt the organization's ability to conduct business. Design customers need assurances that a design offers some protection against business data and other resources getting stolen, lost, or damaged.

#### 13.2.1 Task: Plan a Security Design with Risk in Mind

The first task in security design is planning. Planning involves analyzing risks and developing requirements. As is the case with most technical design requirements, achieving security goals means making tradeoffs. Security implementations can add to the cost of deploying and operating a system. Strict security policies can also affect the productivity of users, especially if some ease-of-use must be sacrificed to protect resources and data. Poor security implementations can annoy users, causing them to think of ways to get around security policies.

#### 13.2.2 Task: Implement Access Control

It is important to implement access control in systems to ensure confidentiality, integrity, and non-repudiation.

#### **Public Key Infrastructure (PKI)**

PKI encompasses the hardware, software, people, policies, and procedures that are used to create, manage, distribute, use, store, and revoke digital certificates. It assists in offering assurance of non-repudiation and secure authentication by utilizing two-factor authentication, which requires the end-user to authenticate with:

- Something they have, AND (token)
- Something they know, OR (password)
- Something they are (biometrics)

---

<sup>27</sup> The Qualification Standards for the Systems Architect are taken from the USCYBERCOM Cyber Work Role Development Plan (CWDP), Systems Architect, and correlate with the Joint Cyberspace Training & Certifications Standards (JCT&CS).

### **Internet Protocol Security (IPSec)**

Internet Protocol Security is a protocol suite that secures IP communications by authenticating and encrypting IP packets of a session. You can significantly enhance the ability of a server to defend against network attacks by requiring IPSec-authenticated, signed, and encrypted communication between computers.

IPSec provides:

- Defense-in-depth against network-based attacks
- Data confidentiality
- Data integrity
- Data origin authentication
- Anti-replay for unicast IP packets sent between trusted hosts

How is risk of attack reduced by IPSec?

- Attack opportunity is reduced to trusted computers
- Attack opportunity is reduced to only the communication paths, protocols, and ports that you specify in an IPSec policy
- Sophisticated attacks based on capturing or manipulating network traffic are greatly reduced through IPSec cryptographic protection

### **Domain Name System Security Extension (DNSSEC)**

Domain Name System Security Extension, or DNSSEC, helps protect the DNS from DNS exploits like cache poisoning.

These attacks can:

- Allow malicious attackers to intercept a users request to access a website
- Send e-mail
- Redirect
- Eavesdrop

It does this by introducing digital signatures into the DNS infrastructure. DNSSEC automatically ensures users are not hijacked.

### **Application Whitelisting**

Application whitelisting is an effective way to deal with the ever-growing problem of malware by only permitting known good files. It flips the antivirus model from a 'default allow' to a 'default deny' for all executable files by creating a list of approved file hashes and only allowing those files to execute.



One of the most significant drawbacks of application whitelisting is the perception of “lockdown” by users. This can impact morale of users. Manageability can also become very complex and require more personnel to manage it.

### **Firewalling**

Firewalling inspects activity behind a firewall and specifies what traffic needs to be let in and out using access lists. There are two types of firewalls:

- Application-level gateways
  - Capable of permitting or rejecting requests based on the content of the network traffic
- Packet filters
  - The functions used for packet filtering are typically available with routers. The router's primary function is to route network traffic based on the source or destination IP addresses, TCP ports, or protocols used.

### **Dynamic Access Control**

Dynamic Access Control lets you identify data by using automatic and manual classification of files. It controls access to files by applying safety-net policies that use central access policies. It also audits access to files by using central audit policies for compliance reporting and forensic analysis.

The Dynamic Access Control feature set is based on an infrastructure that includes:

- A new authorization and audit engine for Windows that can process conditional expressions and central policies
- Kerberos authentication support for user claims and device claims
- Improvements to the File Classification Infrastructure (FCI)
- Rights Management Services (RMS) extensibility supports

## 14. PROVIDE INPUT TO THE IA C&A PROCESS

**Qualification Standard:** Provide input to the IA C&A process activities and related documentation.<sup>28</sup>

### 14.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 14.2. Implementation

In order to operate, each DoD information system must be certified and accredited using a standard set of activities defined within the *Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)*, *DoDI 8510.01*.

#### 14.2.1 Task: Identify the DIACAP's Purpose and its Importance in Protecting DoD Information and Information Systems

The DIACAP establishes the standard certification and accreditation process for DoD information systems. Information systems cannot operate if they are not accredited. To be authorized to operate, DoD information systems must meet the requirements of key information assurance, or IA, policy and guidance. The DIACAP implements the *Federal Information Security Management Act (FISMA)*, *DoDD 8100.1*, *Global Information Grid*<sup>29</sup> *Overarching Policy*, *DoDD 8500.01E*, *Information Assurance*, and *DoDI 8500.2*, *Information Assurance Implementation* by establishing an IA certification and accreditation process for authorizing the operation of DoD Information Systems. The DIACAP is a formal and standard set of activities and tasks that leads to the operation of DoD Information Systems, and the DIACAP defines the management structure for certification and accreditation (C&A). Once an information system has been accredited using the DIACAP, the system's information assurance posture must be maintained throughout the system's life cycle.

#### 14.2.2 Task: Identify the Interrelationship of the DIACAP and its Implementation Tools

In the past, C&A of DoD information systems was system-focused. With the rapid change in technology and the increasing interconnectedness of systems, the need to expand C&A efforts across networks became essential. The DIACAP supports the

---

<sup>28</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

<sup>29</sup> The Global Information Grid, or GIG, is now known as the DoD Information Network, or DODIN.

transition to a network-centric C&A approach that protects and defends the DoDIN. The DIACAP accomplishes this by providing a standard C&A approach that manages and disseminates enterprise standards and guidelines for IA design, implementation, configuration, validation, operational sustainment, and reporting. The DIACAP applies to all systems owned, controlled, or operated on behalf of the DoD, and facilitates a dynamic environment. Following the DIACAP ensures the secure operation of defense information systems and networks.

The implementation of DIACAP is made up of three components. The first component is the DIACAP instruction. Use of the DIACAP is mandatory for all DoD information systems. The second component is a web-based DoD resource that provides the most current requirements, guidance, and tools known as the DIACAP Knowledge Service, or KS. The DIACAP Knowledge Service is the official DoD source for guidance regarding the implementation and execution of the DIACAP. The third component is an automated C&A tool used to electronically document and record the certification activity and the security status of the DoD information systems. The Enterprise Mission Assurance Support Service (eMASS) is the DoD sponsored and recommended tool, but DoD Components may select another DIACAP-conforming automated C&A application or tool to support the Component's implementation of the DIACAP.

#### 14.2.3 Task: Understand Enterprise Risk Management

The C&A process enables DoD IA professionals to manage the risk to the DoD system's operation. If proper IA implementation is validated, the certification can be completed. At the end of the accreditation determination, if the level of residual risk is acceptable, the system is accredited.

Risk management is a critical factor in C&A. Risk to information systems within the DoD is managed at the enterprise level. Risk assessments are conducted DoD-wide, at the mission area (MA), DoD Component, and information system levels as part of an enterprise process for identifying, implementing, and managing IA capabilities and services. IA capabilities and services are expressed as IA controls as defined in DODI, 8500.2. IA controls are maintained through a DoD-wide configuration control and management (CCM) process that considers the DoDIN architecture and risk assessments. The DIACAP ensures that the IA controls are implemented, tested, validated, and maintained. The applicability of IA controls to a specific system is based on the system's mission assurance category (MAC), and the sensitivity of the information process by the system, expressed as the system's Confidentiality Level. The implementation and validation of IA controls create the baseline of information assurance and are the basis of the system's certification and accreditation. When the baseline IA controls are properly applied, correctly configured, tested, and validated there is a reasonable assurance that the information system will operate at an acceptable level of risk. This assurance is a major factor in the decision to provide the system's accreditation, called an "authorization to operate," or ATO. It is essential that the appropriate MAC and Confidentiality Level are identified so that the appropriate IA controls are used.

#### 14.2.4 Task: Assign DoD MAC and Confidentiality Level

DoDD 8500.01E mandates that all DoD information systems be assigned a mission assurance category and confidentiality level by the DoD Component. A system's MAC reflects the importance of information to DoD goals and objectives, particularly the warfighter's combat mission. The MAC assigned to a system determines the minimum operational requirements for its availability and integrity. There are three mission assurance categories:

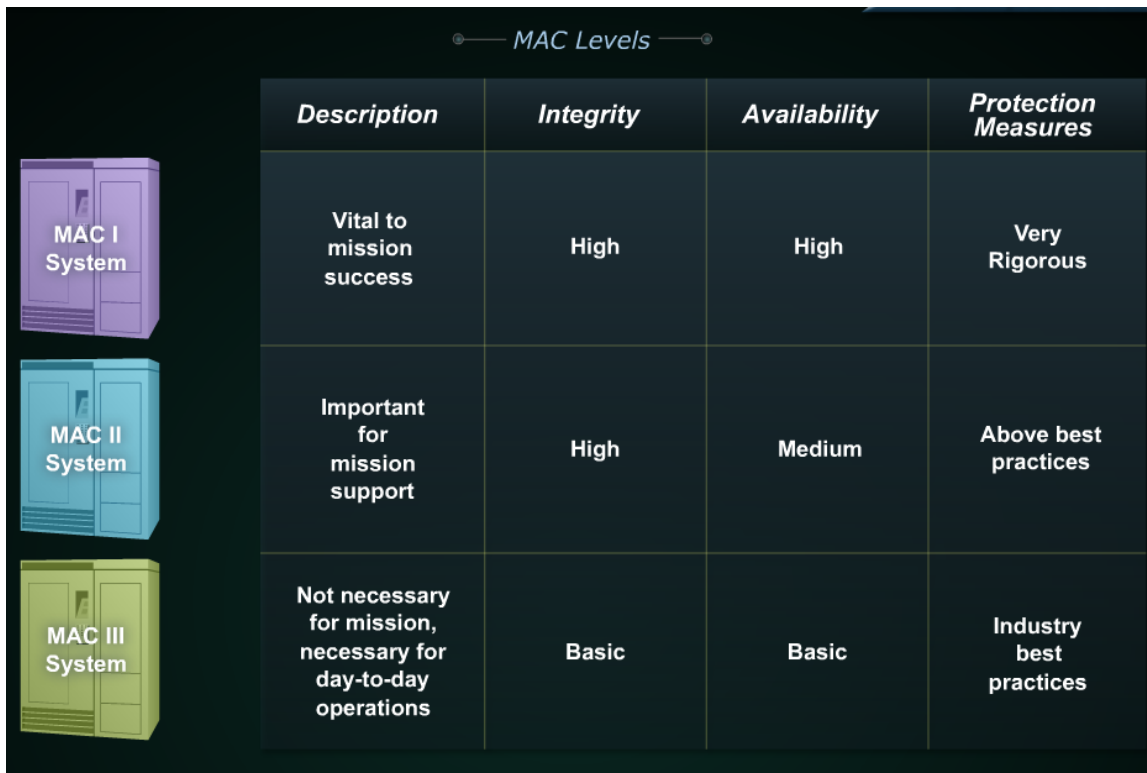
- MAC I
- MAC II
- MAC III

MAC I systems handle information vital to the operational readiness of effectiveness of deployed or contingency forces. Because the loss of MAC I data would cause severe damage to the successful completion of a DoD mission, MAC I systems must maintain the highest levels of both integrity and availability and use the most rigorous measures of protection.

MAC II systems handle information important to support of deployed and contingency forces. The loss of MAC II systems could have a significant negative impact on the success of the mission or operational readiness. The loss of integrity of MAC II data is unacceptable; therefore, MAC II systems must maintain the highest level of integrity. The loss of availability of MAC II data can be tolerated only for a short period of time, so MAC II systems must maintain a medium level of availability. MAC II systems require protective measures above industry best practices to ensure adequate integrity and availability of data.

MAC III systems handle information that is necessary for day-to-day operations, but not directly related to the support of deployed or contingency forces. The loss of MAC III data would not have an immediate impact on the effectiveness of a mission or operational readiness. Since the loss of MAC III data would not have a significant impact on mission effectiveness or operational readiness in the short term, MAC III systems are required to maintain basic levels of integrity and availability. MAC III systems must be protected by measures that are considered industry best practices.

For a visual representation of how to choose the appropriate MAC level, refer to the figure below:

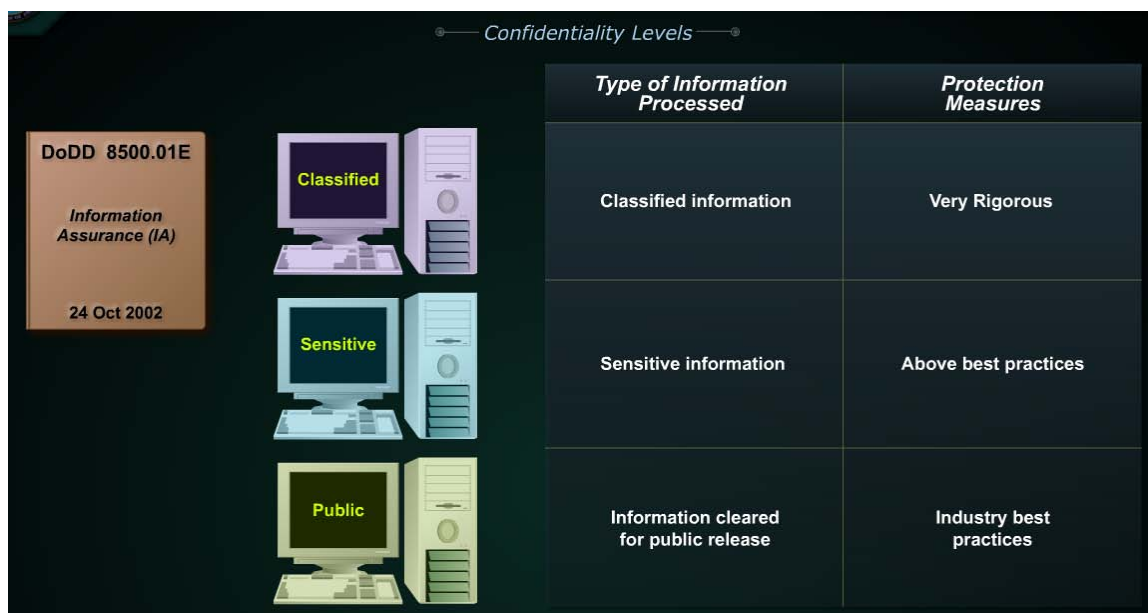


MAC Levels				
	Description	Integrity	Availability	Protection Measures
MAC I System	Vital to mission success	High	High	Very Rigorous
MAC II System	Important for mission support	High	Medium	Above best practices
MAC III System	Not necessary for mission, necessary for day-to-day operations	Basic	Basic	Industry best practices

**Figure 14-1: Choosing the Appropriate MAC Level**

In addition to being assigned a mission assurance category, DoDD 8500.01E requires that each DoD system be assigned a confidentiality level. The confidentiality level is based on the classification or sensitivity of the information the system stores, processes, or transmits. In other words, the confidentiality level depends on whether the system processes classified information, sensitive information, or information that has been cleared for public release. There are three confidentiality levels: classified, sensitive, and public. Systems that process classified information are required to use the most stringent protection measures to protect the classified information processed, stored, or transmitted by that system. Systems that process sensitive information, also known as controlled unclassified information (CUI), require protection measures above best practices to protect that information. Systems that process information that is explicitly cleared for public release require protective measures that are consistent with industry security best practices.

For a visual representation of how to choose the appropriate confidentiality level, refer to the figure below:



**Figure 14-2: Choosing the Appropriate Confidentiality Level**

#### 14.2.5 Task: Implementing IA Controls

A DoD system's assigned mission assurance category and confidentiality level identifies a specific set of required IA controls. An IA control is defined as an objective condition of integrity, availability, or confidentiality that is achieved by applying specific safeguards or regulating specific activities. For example, on a MAC II system, backup copies of all critical software, such as the operating system, should be stored either in a fireproof container or at an offsite location. This IA control provides a condition of availability for the MAC II system. DoD IA controls are organized into eight subject areas. The IA controls in each of these subject areas must have certain characteristics. An IA control must be something that can be tested. You can validate if there are backup copies of all critical software stored in an appropriate location. Also, compliance with the control must be measurable. To continue our previous example, you can determine if there is compliance or non-compliance with the requirement to safely store backup copies of critical software. Additionally, implementation of IA controls must be actions or activities that can be assigned to an individual. One person can be assigned responsibility for making backup copies of software and storing it in the correct location. Finally, because IA controls are assignable, there is accountability for keeping DoD systems secure.

One of the benefits of the DIACAP is that assigned IA controls can be inherited. Inheritance allows two or more systems to share IA controls and their validation results and compliance status for the purpose of C&A. Through inheritance, an existing IA control and its compliance status extends from an originating information system to a receiving information system. For example, if a system is located on a military base and connects to the base's network of information systems, the IA controls of the base's

systems can be inherited. Inheritance eliminates the need to duplicate the testing and documentation of inherited IA controls.

#### 14.2.6 Task: Explain DIACAP Enterprise Governance

The DIACAP establishes a governance structure that assigns certification and accreditation responsibility from the DoD-level to the local, individual information system. This structure synchronizes and integrates DIACAP activities across all levels of the DoD and DODIN areas, or DODIN MAs; all aspects of the IT lifecycle; and logical and organizational entities. The governance structure is divided into three major areas: an accreditation structure, a configuration and control and management structure, and a certification and accreditation process structure. The accreditation structure determines who is responsible for accreditation. The DIACAP CCM structure is responsible for ensuring that a secure IA posture is maintained when there are changes to the DODIN or enterprise-wide requirements. CCM is the responsibility of the DIACAP Technical Advisory Group (TAG). Not surprisingly, the C&A Process structure is where certification and accreditation activities originate.

#### 14.2.7 Task: Identify Key Players Involved in DIACAP Execution

DoD Components have several certification and accreditation responsibilities. Specifically, the DoD Component Heads must ensure that the DIACAP is implemented and that all information systems under their purview are in compliance. The DoD Component Chief Information Officer, or CIO, ensures that the IA controls are being implemented through the DIACAP throughout a system's life cycle. The DoD CIO also ensures that the C&A status of information systems are visible to the Assistant Secretary of Defense for Networks & Information Integration, or ASD (NII), and the PAAs. The DoD Component SIAO leads his or her Component's C&A effort, enforces the C&A process, and tracks C&A status of the Component's information systems.

There is a team of IA professionals that works together to determine whether an information system is operating at an acceptable level of risk:

**DAA** - the official who has the authority to accredit a system and formally assume responsibility for operating a system

**CA** - the official who has the authority and responsibility for certifying the DoD Component's information systems. Either the CA or the CA's designated representative makes a certification recommendation to the DAA.

**Program Manager (PM)** - responsible for planning and budgeting for the implementation, validation, and sustainment of the IA controls throughout the information system's lifecycle. In this role, the PM, sometimes called the System Manager, implements the DIACAP for assigned DoD information systems.

**User Representative** - represents the operational interests of the user community. He or she provides critical feedback on the acceptability and feasibility of system security implementation in field operation.

**Validator** - responsible for conducting validation procedures. Specific validation duties and requirements should be defined by the DoD Component.

**Information Assurance Manager (IAM)** - responsible for the information assurance program of a DoD information system or organization. The IAM ensures that systems are developed with and operate at an acceptable level of risk, and supports the PM in the implementation of the DIACAP.

**Information Assurance Officer (IAO)** - is responsible for ensuring that the appropriate information assurance posture is maintained for the information system or organization. The IAO ensures that all users have the requisite security clearances and need-to-know authorization, and are aware of their IA responsibilities before being granted access to a DoD information system.

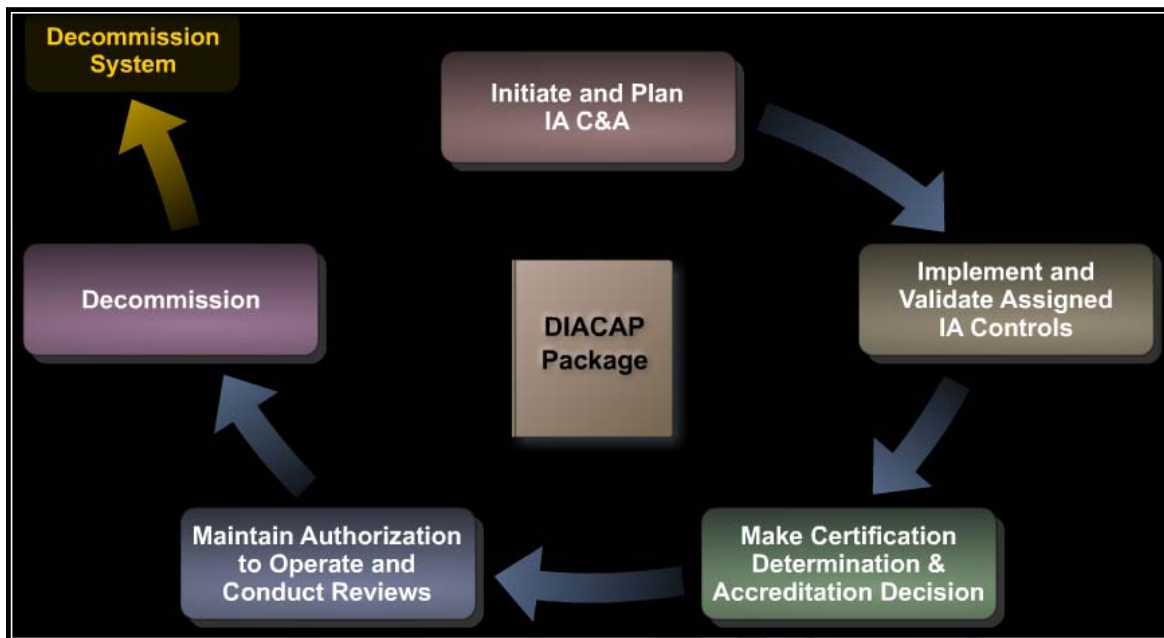
#### 14.2.8 Task: Identify the DIACAP Activities

The DIACAP is comprised of five main activities. IA must be built into the acquisition of a system, and DIACAP activities are initiated from the start and continue throughout the system's lifecycle. The first activity in the DIACAP process is to initiate and plan IA C&A. The second activity is to implement and validate assigned baseline IA controls. In the third activity, the certification determination and accreditation decision are made. The fourth activity begins after the accreditation decision is made. The system must continue to operate at an acceptable level of risk to maintain its accreditation. Periodic reviews are conducted to ensure that the system is operating within the baseline and the IA controls are implemented correctly. The fifth and final activity in the DIACAP process is to decommission, or retire, the system. Throughout DIACAP activity, the DIACAP package is developed and maintained throughout a system's lifecycle. The components of the DIACAP package are used to make the accreditation decision.

#### 14.2.9 Task: Identify the DIACAP Package Components

The DIACAP package is developed through DIACAP activity and maintained throughout a system's lifecycle. Implementing the activities of the DIACAP generates the Comprehensive Package. The Executive Package contains the minimum information necessary for an accreditation decision. The DIACAP package is not meant to describe a single fixed document format. Each DAA will determine what information is necessary to make an accreditation decision. See the figure below for a visual representation of DIACAP package components.





**Figure 14-3: DIACAP Package Components**

#### 14.2.10 Task: Understand how IA C&A is Planned and Initiated

Initiating and planning the IA C&A includes registering the system with the governing DoD Component IA Program. System registration establishes the relationship between the DoD information system and the governing DoD IA Program. The System Identification Profile (SIP) is generated during the registration process and becomes part of the DIACAP package. Specific registration requirements may change. Requirements are published in the DIACAP Knowledge Service. Initiating and planning the IA C&A also includes assigning IA Controls. The IA Controls are assigned based on the Mission Assurance Category and the Confidentiality Level, both discussed in Section 14 of this document. An important aspect of initiating and planning IA C&A is assembling the DIACAP team. The DIACAP team is composed of members responsible for implementing the DIACAP for a DoD information system. Finally, initiating and planning the IA C&A includes initiating the information system's DIACAP implementation plan (DIP), which becomes part of the DIACAP package. The DIP contains the information system's assigned IA Controls, implementation status, responsible entities, resources, and estimated completion date for each assigned IA Control.

#### 14.2.11 Task: Understand how IA Controls are Validated and Assigned

Implementing and validating assigned IA controls includes all tasks related to executing the DIACAP implementation plan. Each assigned IA control is implemented according to the requirements for that IA control as described in the DIACAP Knowledge Service. Validation activities include all tasks related to executing the validation procedures for each assigned IA control. Each validation procedure describes the required preparatory

steps and conditions, the actual validation steps, the expected results of the validation, and the criteria and the protocols for recording actual results. An IT Security Plan of Action and Milestones (POA&M) is also part of the DIACAP package. The validation results are then compiled in the DIACAP scorecard. The DIACAP scorecard is a summary report that shows the implementation status of a DoD information system's assigned IA controls. The DIACAP scorecard supports or conveys a certification determination and/or accreditation decision. Information is added to the scorecard throughout the C&A process.

#### 14.2.12 Task: Understand how Determination and C&A Decision is Made

The third DIACAP activity is the certification determination and accreditation decision. The certification determination is made by the Certifying Authority and is based on the validation of actual results from the implementation and testing of the assigned IA controls. The certification considers the overall reliability and viability of the information system, and how the information system behaves in the larger information environment. The Certifying Authority validates the system's compliance with IA controls, identifies and assesses the risks with the operating system, and assesses the cost to correct or minimize any IA security weaknesses. The Certifying Authority then makes the certification determination available to the DAA for input into the accreditation decision. An accreditation decision always requires a certification determination. If an urgent need requires the rapid introduction of a new DoD information system, the validation activity and certification determination are still required. The accreditation decision comes from the DAA and is an official designation made in writing by signing the DIACAP Scorecard. The DAA's authorization is based on a balance of mission or business need, protection of information being processed, and the protection of the information environment. Under the DIACAP, the DAA has the option of granting any one of four possible accreditation decisions: Authorize to Operate, Interim Authorization to Operate, Interim Authorization to Test, or Denial of Authorization to Operate.

#### 14.2.13 Task: Understand How to Maintain Authorization to Operate

Once an information system is certified and accredited, it must maintain an acceptable IA posture to continue its authorization to operate. The IAM is primarily responsible for monitoring systems for a change in IA posture. To determine if a system's IA posture has changed, the IAM must maintain situational awareness. The IAM does this by monitoring for security-related events and system configuration changes that may negatively impact the system's IA posture. The IAM also assesses the quality of IA controls implementation against performance indicators such as security incidents, exercises, and operational evaluations. When necessary, the IAM indicates actions to improve or restore IA posture. The IAM may schedule revalidation of any or all IA controls. The DAA may direct the IAM to schedule revalidation, or the IAM may do so independently. The IAM also conducts reviews of selected IA controls annually. The DAA receives a written statement from the IAM that either confirms the effectiveness of assigned IA controls and their implementation, or recommends changes. The DAA

reviews the IAM statement together with the Certifying Authority and determines if a change in accreditation status is required.

In addition to potential changes in accreditation status that are triggered by annual reviews and the schedule determination of accreditation decisions, changes may be event-driven. The DAA may downgrade or even revoke an accreditation at any time due to risk conditions or concerns. Systems that have an ATO must be recertified and reaccredited once every three years. However, the results of validation tests of IA controls conducted during an annual review may be used in the recertification and re-accreditation process.

#### 14.2.14 Task: Understand Decommissioning of a DoD Information System

When a DoD information system is removed from operation, a number of IA-related events are required. These events include assessing impact of the decommissioning to other systems, updating records to reflect the decommissioning, and disposing of the DIACAP registration and system-related data. Decommission requirements and procedures change over time. These changes are published in the DIACAP Knowledge Source.

## 15. ENSURE CONSISTENCY WITH DOD ARCHITECTURE

**Qualification Standard:** Ensure that acquired or developed systems and architectures are consistent with DoD Component level IA architecture.<sup>30</sup>

### 15.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/)

### 15.2. Implementation

The Systems Architect should assist in ensuring that all incorporated IA products, and IA-enabled IT products must be validated and certified in accordance with the Common Criteria<sup>31</sup>.

#### 15.2.1 Task: Ensure all IA and IA-enabled IT Products are Validated and Certified in Accordance with the Common Criteria (CC)

At the enterprise level, implementation-independent specifications for IA and IA-enabled IT products are provided in the form of protection profiles (PP). Protection profiles are developed in accordance with the Common Criteria within the National Information Assurance Partnership (NIAP) framework.

All Business Systems Modernization (BSM) IA and IA-Enabled Commercial off-the-shelf (COTS) products purchased after July 1, 2002 must be validated and certified in accordance with the CC regardless of their mission assurance category or robustness levels<sup>32</sup>.

More information is available at the following websites:

- International Common Criteria for Information Technology Security Evaluation (<http://www.commoncriteria.org/>)
- National Information Assurance Partnership's (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), (<http://niap.nist.gov/>)

---

<sup>30</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

<sup>31</sup> Common Criteria - Common Criteria is used as the basis for a Government driven certification scheme and typically evaluations are conducted for the use of Federal Government agencies and critical infrastructure.

<sup>32</sup> DoDI 8500.2, para E3.2.5

- The National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptomodule Validation Program (CMVP), (<http://csrc.nist.gov/cryptval/>)<sup>33</sup>.

A protection profile (PP) is a generic set of security requirements for a specific technology e.g. firewalls. Acquisition of a product is restricted to those products that have already been certified under a US government approved PP or those that are submitted for evaluation and validation by the vendor prior to purchase. The US only recognizes products certified for EALs 1-4 outside the US. Products requiring EAL 5 and higher must be certified by the NIAP CCEVS (US CC evaluation scheme).

More information is available at the following websites:

- <http://niap.nist.gov/cc-scheme/PPRegistry.html> (Validated and draft US government PP)
- <http://niap.nist.gov/cc-scheme/ValidatedProducts.html> (Validated NIAP CCEVS CC products)
- <http://niap.nist.gov/cc-scheme/InEvaluation.html> (Products in evaluation through NIAP CCEVS)
- [http://www.commoncriteria.org/introductory\\_overviews/CCIntroduction.pdf](http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf)
- (For details on each Evaluation Assurance Level (EAL), see [http://www.commoncriteria.org/introductory\\_overviews/CCIntroduction.pdf](http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf))

If a PP exists for a specified technology but no validated product/s exist under this PP within the NIAP CCEVS, the vendor needs to do the following:<sup>34</sup>

1. Submit their product/s for CC evaluation and verification prior to the purchase being executed
2. Submit a security target (implementation dependent specification of the security required, both functionality and assurance) for the product/s against the approved US government PP
3. The acquiring DoD organization may also optionally purchase a CCRA validated product from the list:

[http://www.commoncriteria.org/index\\_ccra\\_registry.htm](http://www.commoncriteria.org/index_ccra_registry.htm) (CCRA validated product registry)

[http://www.commoncriteria.org/protection\\_profiles/index.html](http://www.commoncriteria.org/protection_profiles/index.html) (CCRA PP registry)

---

<sup>33</sup> The NIST FIPS Cryptomodule Validation (CMV) program specifically validates products containing cryptographic modules. Not all IA and IA-enabled COTS products contain such modules.

<sup>34</sup> DoDI 8500.2, para E3.2.5.2

If no PP exists for a specified technology and the acquiring organization chooses not to purchase a product evaluated by NIAP CCEVS or CCRA, then the acquiring organization must require proof from the vendor that:<sup>35</sup>

1. The vendor submitted their product/s for CC evaluation and verification at a DAA approved EAL prior to the purchase being executed and
2. The vendor submitted a security target describing the security attributes of their product(s).
3. The acquiring organization based on their needs, robustness level and mission will recommend an EAL for the required IA or IA-Enabled product for their organization. This implies that a given product that satisfies an EAL in one DoD program may need to satisfy a different EAL in another DoD program.

If the acquiring organization anticipates using subsequent versions of an evaluated product, they need to specify wording in the original contract that requires the vendor of the product to keep subsequent versions of their product/s validated through the NIAP CCEVS Maintenance Program ([http://niap.nist.gov/cc-scheme/Pub6\\_v1.pdf](http://niap.nist.gov/cc-scheme/Pub6_v1.pdf)), or the CCRA Maintenance Programs ([http://www.commoncriteria.org/review\\_docs/docs/AMAv09.pdf](http://www.commoncriteria.org/review_docs/docs/AMAv09.pdf))<sup>36</sup>.

---

<sup>35</sup> DoDI 8500.2, para E3.2.5.3

<sup>36</sup> DoDI 8500.2, para E3.2.5.4

## 16. PERFORM TECHNICAL REVIEW

**Qualification Standard:** Perform security reviews and identify gaps in security architecture.<sup>37</sup>

### 16.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 16.2. Implementation<sup>38</sup>

According to the *Defense Acquisition Guide*, a technical review of systems must be completed with their key results or impact(s) to design and any related recommendations and status of actions taken being published in a Technical Review Table.

#### 16.2.1 Task: Summarize Plans for Conducting Technical Review

Summarize the PMO's plans for conducting each technical review with particular emphasis and detail on those technical reviews planned in the program's next acquisition phase. Identify which program office position is responsible for the overall conduct of system-level and/or key subsystem-level technical reviews. A diagram of the process with the objective timeframes for each activity before, during, and after the technical review may prove useful.

Identify who or what team has responsibility, authority, and accountability for determining:

- Whether/when technical review entry criteria have been met
- What action items are to be tasked
- That tasked action items have been closed appropriately
- That technical review exit criteria are met

If not already addressed, identify the role of the program manager, LSE/CSE, and Technical Review Chair in the technical review process.

A sample Technical Review Table appears below:

---

<sup>37</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

<sup>38</sup> OPR: ADASD (Systems Engineering), *Systems Engineering Plan (SEP) Outline, Version 1.0*, 20 April 2011

Table 16-1: Sample Technical Review Table

<b>XXX Details Area</b>	<b>XXX Review Details</b> (For this acquisition phase, fill out tailored criteria, etc.)
<b>Chairperson</b>	Identify the Technical Review Chair (Normally the LSE)
<b>PMO Participants</b>	Identify Positions/functions/IPTs within the program offices which are anticipated to participate. (Engineering Leads; Risk, Logistics, and Configuration Managers, Defense Contracting Management Agency (DCMA) Rep., and Contracting Officer, etc.)
<b>Anticipated Stakeholder Participant Organizations</b>	Representatives (stakeholders) from Service SE and Test, OSD SE and Developmental Test and Evaluation (DT&E), FoS/SoS, and the User
<b>Anticipated Peer and Program-Independent SME Participant Orgs.</b>	Identify Organizations which can provide a peer perspective and participants who will provide an independent assessment of how well the program is progressing but which have no stake in the program's success.
<b>Purpose (of the review)</b>	Describe the main purpose of the review and any specific SE goals
<b>Entrance Criteria</b>	Identify tailored Entrance Criteria
<b>Exit Criteria</b>	Identify tailored Exit Criteria
<b>Products/Artifacts (from the review)</b>	<p>List expected products from the technical Review (for example)</p> <ul style="list-style-type: none"> <li>• Established system allocated baseline</li> <li>• Updated risk assessment for EMD</li> <li>• Updated Cost Analysis Requirements Document (CARD) or CARD-like document based on system allocated baseline</li> <li>• Updated program schedule including system and SW critical path drivers</li> <li>• Approved LCSP updating program sustainment development efforts and schedules</li> <li>• Draft Post-PDR Report (MDAPS)</li> </ul>



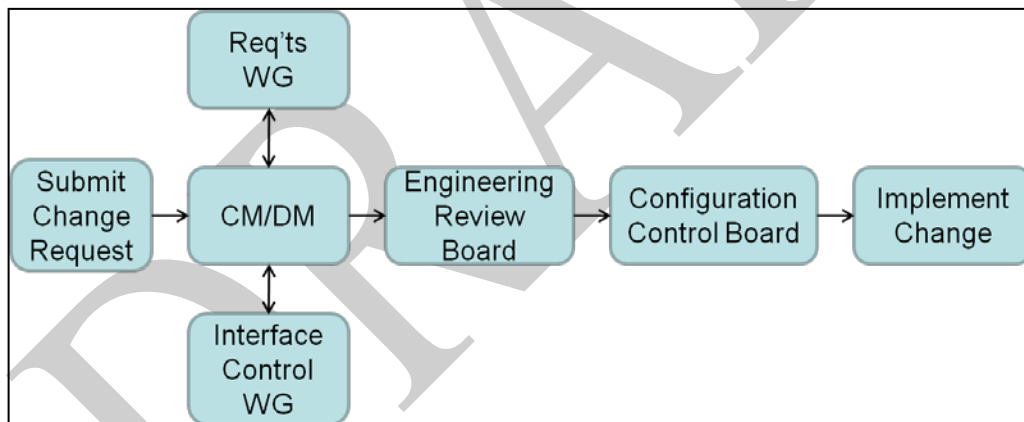
### 16.2.2 Task: List and Describe Planned or Established Artifacts

For each baseline established at a technical review, list and describe the planned or established artifacts (if not already identified in Section 4.4). Typically, at a minimum, the following apply:

- System Functional Review (SFR) = Functional Baseline = System Specification and external specifications
- Preliminary Design Review (PDR) = Allocated Baseline = Item Performance Specification for each end product, internal interface specifications, and allocated external interface specifications, and preliminary drawings
- Critical Design Review (CDR) = Initial Product Baseline = Item Detail Specification for each end product, internal interface specifications, allocated external interface specifications, and detailed (build-to) drawings

### 16.2.3 Task: Provide a Configuration Management (CM)/Control Process Description

Provide a process diagram of how the program will maintain configuration control of its baselines. Identify when in the acquisition lifecycle the program will assume initial and full configuration control of its baselines.



**Figure 16-1: Sample Process Diagram**

**Roles, Responsibilities, and Authorities** - Summarize the roles, responsibilities, and authorities within the CM process. If this includes one or more configuration boards, describe the hierarchy of these boards, their frequency, who (by position) chairs them, who participates, and who (by position) has final authority in each.

**Configuration Change Process** – Outline the process the program will use to change the technical baseline/configuration and specifically address:

- How changes to a technical baseline are identified, evaluated, approved/disapproved, recorded, incorporated, and verified;

- How product information is captured, maintained, and traced back to requirements;
- How requirements for in-service configuration/design changes are determined and managed/controlled; and
- How internal interfaces are managed and controlled.

**Classification of Changes** – Define the classification of changes (Class 1, Class 2, etc.) applicable to the program.

**Roles, Responsibilities and Authorities** – Identify by position who in the CM process is responsible for determining the classification of a change and who (by position) verifies/confirms/approves it.

## 17. PRIORITIZE CAPABILITIES AFTER A CATASTROPHY

**Qualification Standard:** Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.<sup>39</sup>

### 17.1. Training

The training courses at the following website include DoD courses offered by various Services and Agencies, and map to the KSAs and the Qualification Standard listed in this section:

[https://powhatan.iiee.disa.mil/specialty\\_courses/](https://powhatan.iiee.disa.mil/specialty_courses/).

### 17.2. Implementation

According to DODI 8500.2, *Subject Area Continuity, Control Number CODP-3, Disaster Recovery and Planning*, A disaster plan must exist that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. Disaster recovery procedures should include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.

#### 17.2.1 Task: Use the Trusted Recovery Methodology to Deter, Detect, and Reduce Impacts to Mission and Functions<sup>40</sup>

In some cases, threat impacts may be mitigated or eliminated through preventative measures that deter, detect, and/or reduce impacts to missions and functions. Where feasible and cost-effective, preventative methods are preferable to actions that may be necessary to recover the normal operations after a disruption. Preventative controls have been identified below to limit any circumstance to inhibit trusted recovery:

Uninterruptible Power Supplies (UPS) provide short-term backup power to all DISANet networking components (including environmental and safety controls).

Air-conditioning system with adequate excess capacity to permit failure of certain components, such as a compressor.

Fire suppression devices, plus fire and smoke detectors, in proper working order and checked bi-annually are installed for operational effectiveness.

DISANet baseline images are backed up weekly and stored in a fire proof safe within a secure area

---

<sup>39</sup> The Qualification Standards for the Systems Architect are taken from the *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, *Systems Architect*, and correlate with the *Joint Cyberspace Training & Certifications Standards (JCT&CS)*.

<sup>40</sup> *DISA, FSO Contingency and Business Continuity (CBCP) and Disaster Recovery Plan (DRP) for the FSO LAN, Version 2*, Release 1, August 2013

Use of enterprise storage services for backing up hardware, firmware, and software inventories such web sites as DEPS, DEE (include OWA from personal computers), DISANet local file server, DISA Records Management, or the DoD Patch Repository.

#### 17.2.2 Task: Use Reconstitution Tactics

Reconstitution addresses those actions and tasks necessary to construct, modify, and/or refurbish a new facility in cases where the contingency situation or event rendered the original facility uninhabitable or required the original facility to be remodeled. The following will be part of reconstitution actions:

1. Define a new infrastructure environment which could be in a new geographical location.
2. Install system hardware, software, and firmware.
3. Establish connectivity and interfaces with network components and external systems.
4. Back-up operational data from contingency systems and upload to restored system.
5. Shut down the contingency system and terminate contingency operations.
6. Notify affected customers and management of reconstituted processing location.
7. Secure, remove, and/or relocate all sensitive/classified materials from the contingency site.
8. Arrange for recovery personnel to return to the reconstituted facility.
9. Initiate a phased resumption of all functions.

#### 17.2.3 Task: Prioritize Essential System Capabilities

##### **Hardware Backups**

The Business Continuity Plan (BCP) team should identify the equipment required to keep the critical functions up and running. This may include servers, user workstations, routers, switches, tape backup devices, and more. The BCP team should plan for the recovery team to use the company's current images, but also have a manual process for building each critical system from scratch with the necessary configurations.

The BCP team also needs to identify how long it will take for new equipment to arrive. The Service Level Agreement (SLA) for the identified vendors needs to be investigated to make sure the company is not further damaged by delays. Once the parameters of the SLA are understood, the team must make a decision between depending upon the vendor and purchasing redundant systems and storing them as backups in case the primary equipment is destroyed.

The team should also identify any legacy devices and understand the risk the organization is facing if replacements are unavailable.

##### **Software Backups**

The BCP team should make sure to have an inventory of the necessary software required for mission-critical functions and have backup copies at an offsite facility. The software that needs to be backed up can be in the form of applications, utilities, databases, and operating systems. The continuity plan must have provisions to back up and protect these items along with hardware and data.

The BCP team should make sure there are at least two copies of the company's operating system software and critical applications. One copy should be stored onsite and the other copy should be stored at a secure off-site location. These copies should be tested periodically and re-created when new versions are rolled out.

#### 17.2.4 Task: Implement Software Escrow

The organization should implement software escrow, which means that a third party holds the source code, backups of the compiled code, manuals, and other supporting materials. A contract between the software vendor, customer, and third party outlines who can do what and when with the source code. This contract usually states that the customer can have access to the source code only if and when the vendor goes out of business, is unable to carry out stated responsibilities, or is in breach of the original contract. If any of these activities take place, then the customer is protected because it can still gain access to the source code and other materials through the third-party escrow agent.

# **SYSTEMS ARCHITECT**

## **Procedure Guide**

### **Appendices**



Version 1 Release 1  
10 JANUARY 2014

DRAFT

This page is intentionally left blank.

DRAFT



## APPENDIX A – NICE TO JCT&amp;CS CROSSWALK

Information from the National Initiative for Cybersecurity Education (NICE) Framework and CYBERCOM's Joint Cyberspace Training and Certification Standards (JCT&CS) were utilized within this document.

**NICE to JCT&CS Crosswalk**

The following table displays a correlation of the Knowledge, Skills, and Abilities (KSA) within both documents that are required to complete the duties of the Server Administrator.

**Table A-1: NICE to JCT&CS KSA Crosswalk**

KSAs for Systems Architect NICE	KSAs for Systems Architect JCT&CS
No comparable KSA	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
No comparable KSA	Knowledge of circuit analysis.
Knowledge of encryption algorithms (e.g., Internal Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Knowledge of computer algorithms.
Knowledge of computer networking fundamentals.	Knowledge of computer networking fundamentals.
Knowledge of encryption algorithms (e.g., Internal Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES])	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE, MD5, SHA, 3DES).
Knowledge of cryptology.	Knowledge of cryptology.
Knowledge of database systems.	Knowledge of database systems.
Knowledge of organization's enterprise information security architecture system.	Knowledge of DoD Component-level IA architecture.

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

<b>KSAs for Systems Architect NICE</b>	<b>KSAs for Systems Architect JCT&amp;CS</b>
Knowledge of enterprise information technology (IT) architecture.	No comparable KSA
Knowledge of the organization's enterprise information technology (IT) goals and objectives.	Knowledge of DoD confidentiality, integrity, and availability requirements.
Knowledge of organization's evaluation and validation requirements.	Knowledge of DoD evaluation and validation requirements.
No comparable KSA	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware.
Knowledge of embedded systems.	Knowledge of embedded systems.
No comparable KSA	Knowledge of existing IA security principles, policies, and procedures.
Knowledge of fault tolerance.	Knowledge of fault tolerance.
Knowledge of how system components are installed, integrated, and optimized.	Knowledge of how system components are installed, integrated, and optimized.
Knowledge of human-computer interaction principles.	Knowledge of human-computer interaction principles.
Knowledge of the Security Assessment and Authorization (SA&A) process.	Knowledge of IA Certification and Accreditation process.
Knowledge of industry-standard and organizationally-accepted analysis principles and methods.	Knowledge of IA or IA-enabled software products.
Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation.	Knowledge of Information Assurance principles and tenets (confidentiality, integrity, availability, authentication, non-repudiation).
Knowledge of information theory.	Knowledge of information theory.
Knowledge of computer algorithms.	Knowledge of mathematics, including algorithms, trigonometry, linear algebra, calculus, and statistics.
Knowledge of microprocessors.	Knowledge of microprocessors.
Knowledge of network access, identity,	Knowledge of network access and

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

<b>KSAs for Systems Architect NICE</b>	<b>KSAs for Systems Architect JCT&amp;CS</b>
and access management (e.g., public key infrastructure [PKI]).	authorization (e.g., public key infrastructure).
Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.
Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP], and directory services (e.g., Domain Name System [DNS])).	Knowledge of network management principles, models, and tools.
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	No comparable KSA
Knowledge of network security architecture, including the application of Defense-In-Depth principles.	Knowledge of network security architecture, including the application of Defense-In-Depth principles.
Knowledge of operating systems.	Knowledge of operating systems.
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Open System Interconnection [OSI], Information Technology Infrastructure Library [ITIL]).	Knowledge of OSI model and underlying networking protocols (e.g. TCP/IP).
Knowledge of parallel and distributed computing concepts.	Knowledge of parallel and distributed computing concepts.
Knowledge of risk management processes, including steps and methods for assessing risk.	Knowledge of risk management processes, including steps and methods for assessing risk.
Knowledge of secure configuration management techniques.	Knowledge of secure configuration management techniques.
Knowledge of security management.	Knowledge of security management.
Knowledge of security system design	Knowledge of security system design tools,

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

<b>KSAs for Systems Architect NICE</b>	<b>KSAs for Systems Architect JCT&amp;CS</b>
tools, methods, and techniques.	methods, and techniques.
Knowledge of software engineering.	Knowledge of software engineering.
Knowledge of systems testing and evaluation methods.	Knowledge of systems testing and evaluation methods.
Knowledge of telecommunications concepts.	Knowledge of telecommunications concepts.
Knowledge of the systems engineering process.	Knowledge of the systems engineering process.
Knowledge of information technology (IT) architectural concepts and frameworks.	Knowledge of various types of computer architectures.
Skill in designing the integration of hardware and software solutions.	Skill in designing the integration of hardware and software solutions.
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes.
Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.
Skill in the use of design modeling (e.g., unified modeling language).	Skill in writing code in a modern programming language (e.g., Java, C++).
Knowledge of interpreted and compiled computer languages.	No comparable KSA
Knowledge of access authentication methods.	No comparable KSA
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	No comparable KSA
Knowledge of server and client operating systems.	No comparable KSA
Knowledge of technology integration	No comparable KSA

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

**SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

<b>KSAs for Systems Architect NICE</b>	<b>KSAs for Systems Architect JCT&amp;CS</b>
process.	
Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	No comparable KSA
Skill in applying and incorporating information technologies into proposed solutions.	No comparable KSA
Knowledge of the methods, standards, and approaches for describing, analyzing, and documenting an organizations, enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DODAF], Federal Enterprise Architecture Framework [FEAF]).	No comparable KSA
Knowledge of Personally Identifiable Information (PII) and Payment Credit Industry (PCI) data security standards.	No comparable KSA
Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures.	No comparable KSA
Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not sue standard information technology [IT]) for safety, performance, and reliability.	No comparable KSA

## APPENDIX B – REFERENCES

The following documents should be referenced as part of the execution of functions in this guide.

- a. *Action Officer's CCRI Preparation Guide, Field Security Operations, Defense Information Systems Agency*
- b. *Cisco Systems Top Down Network Design, A Systems Analysis Approach to Enterprise Network Design, 2011*
- c. *Defense Information Systems Agency, Field Security Operations, Contingency and Business Continuity (CBCP) and Disaster Recovery Plan (DRP) for the Field Security Operations (FSO) Local Area Networks (LAN), Version 2 Release 1, August 2013*
- d. *Department of Defense Directive (DoDD) 3020.26, Department of Defense Continuity Programs, 9 January 2009*
- e. *Department of Defense Instruction (DoDI) 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007*
- f. *Department of Defense Instruction (DoDI) 8500.2, Information Assurance (IA) Implementation, 6 February 2003*
- g. *DoD Deputy Chief Information Officer's DoD Architecture Framework, Version 2.02, August 2013*
- h. *DoD External Interoperability Plan, Version 1.0, Joint Interoperability Test Command, December 2013*
- i. *DoD PKI Interoperability Test Plan, Version 2.0, Joint Interoperability Test Command, December 2013*
- j. *Element K CompTIA Network + Certification (2009 Objectives), Volume 1, January 2009*
- k. *Harris, Shon CISSP, All in One CISSP Exam Guide, 6<sup>th</sup> Edition, 2013*
- l. *International Common Criteria for Information Technology Security Evaluation, <http://www.commoncriteria.org/>, December 2013*
- m. *Joint Interoperability Test Command, PKI Infrastructure Home, [http://jitc.fhu.disa.mil/pki/pke\\_lab/partner\\_pki\\_testing/partner\\_pki\\_status.html](http://jitc.fhu.disa.mil/pki/pke_lab/partner_pki_testing/partner_pki_status.html), December 2013*
- n. *National Information Assurance Partnership's (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), <http://niap.nist.gov/>, December 2013*
- o. *Office of the Secretary of Defense, Systems Engineering Plan Format, 20 April 2011*
- p. *USCYBERCOM Concept of Operations (CONOPS) Joint Cyberspace Training and Certification Standards (JCT&CS) V.1.2, 7 February 2012*

- q. *USCYBERCOM Cyber Work Role Development Plan (CWDP)*, 6 December 2010

DRAFT

## APPENDIX C – TRAINING RESOURCES IN THE DOD

**Training**

The following table lists the available training within DISA and FedVTE. For a complete list of courses across the DoD that are organization-specific, refer to [https://powhatan.iie.disa.mil/specialty\\_courses/catalog.html](https://powhatan.iie.disa.mil/specialty_courses/catalog.html).

**Table C-1: Training Course List**

Training Course Name	Method of Delivery
A+ Essentials 2009	eLearning
ActionScript and Multimedia in Flash CS4	eLearning
Administering & Securing Exchange 2010	Classroom
Administering & Securing Windows 2008	Classroom
Advanced PCAP Analysis and Signature Development (APA)	FedVTE
Agile Programming and Testing	eLearning
Ajax Basics	eLearning
ANSI C Programming	eLearning
Applications Security in the Development Life Cycle	IASE Website
Assessing Network Vulnerabilities	Classroom
Backing up and Restoring Databases	eLearning
Black-Box Software Testing Techniques	eLearning
Business Continuity, Disaster Recovery, Security Training, and Forensics	eLearning
C++ Programming	eLearning
CCNA Security	FedVTE
CCNA Security	FedVTE
Centaur SiLK Traffic Analysis	FedVTE
Certified Ethical Hacker (CEHv7)	FedVTE



**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Training Course Name	Method of Delivery
CISA	eLearning
CISCO ASA Adaptive Security Appliance	eLearning
CISCO CVOICE 8.0	eLearning
CISCO DESGN 2.1	eLearning
CISCO FIREWALL 2.0	eLearning
CISCO ICND	eLearning
CISCO IINS	eLearning
Cisco Network Security 1	FedVTE
Cisco Network Security 2	FedVTE
CISCO SECURE	eLearning
CISM	eLearning
CISSP 2012	eLearning
CompTIA A+ Prep	FedVTE
CompTIA Network +	eLearning
CompTIA Network + N10-005 Certification Prep	FedVTE
CompTIA Security + 2008	eLearning
CompTIA Security + Prep	FedVTE
Computer Network Defense	IASE Website
Configuration Management, Risks, and Incidents in Software Testing	eLearning
Configure Windows 2008 AD	Classroom
Configuring Network Connectivity in Windows 7	eLearning
Creating Databases	eLearning
Cryptography and Public Key Infrastructures	eLearning

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

<b>Training Course Name</b>	<b>Method of Delivery</b>
Cyber Law 1	IASE Website
Cyber Law 2	IASE Website
Cyber Risk Management for Managers	FedVTE
Cyber Security Overview for Managers	FedVTE
CyberProtect	IASE Website
Cybersecurity Compliance Validation (CCV)	FedVTE
Data Management, Localization, and Encryption in Linux	eLearning
Data Management, Localization, and Encryption in Linux	eLearning
Database Diagnostics	eLearning
DIACAP	IASE Website
DISA HBSS Supplemental Content	FedVTE
DNSSEC Training Workshop	FedVTE
DoD IA Boot Camp	Classroom
DoD Information Assurance Awareness	IASE Website
DoD Information Assurance Cyber Awareness Challenge	IASE Website
DoD NetOps	FedVTE
Email Authentication Workshop	FedVTE
eMass	Classroom
EMC ISM v2: RAID and Intelligent Storage Systems	eLearning
Emerging Cybersecurity Threats (2010)	FedVTE
Enhancing IA through Physical Security	IASE Website
Exchange Server 2010 SP1: High	eLearning

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Training Course Name	Method of Delivery
Availability	
Footprinting, Scanning, and Enumerating	eLearning
Fundamentals of Software Testing	eLearning
Getting Started with ADO.NET 4 Connections and Commands using C# 2010	eLearning
Getting Started with Software Programming	eLearning
IA for DoD Auditors and IGs	IASE Website
Implementing and Securing VoIP	Classroom
Implementing Network Security	Classroom
Incident Handling and Forensics	Classroom
Industry Overview: Information Technology	eLearning
Information Assurance Awareness Shorts	IASE Website
Information Assurance for Professionals Shorts	IASE Website
Information Assurance Policy and Technology (IAP&T)	IASE Website
Information Risk Management: Program Framework and Risk Assessment	eLearning
Information Security Awareness	eLearning
Information Security Risk Assessments	Classroom
Internet Security Fundamentals	FedVTE
Intro to IPv6	FedVTE
Introducing Agile Software Development	eLearning
Introducing User-Centered Design	eLearning
Introduction to HTTP/HTTPS Analysis	FedVTE

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Training Course Name	Method of Delivery
Introduction to Software Programming Design	eLearning
Introduction to Software Programming Design	eLearning
Introductory Control Systems Security (ICSST)	FedVTE
IPv6 for Security Professionals	Classroom
IPv6 Security	FedVTE
ISA Server 2004 Management and Clientele	eLearning
ISACA Certified Information Security Manager	FedVTE
ISACA Certified Information Systems Auditor	FedVTE
ISC2™ CAP® Prep	FedVTE
ISC2™ CISSP	FedVTE
ISC2™ CISSP	FedVTE
IT Project Management Essentials	eLearning
ITIL® 2011 Edition OSA	eLearning
ITIL® V3 OSA	eLearning
Java Programming with J2SE 5	eLearning
Java Programming with Java SE 6.0	eLearning
Java SE7 Fundamentals	eLearning
Java SE7 New Features	eLearning
Java SE7 Professional	eLearning
JavaScript	eLearning
JavaScript Language Basics	eLearning

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

<b>Training Course Name</b>	<b>Method of Delivery</b>
Junior Level LPIC- 1 Exam 102	eLearning
Microsoft Windows 8	eLearning
Microsoft Windows Server 2003	eLearning
Microsoft.NET Framework 4	eLearning
Mobile IP	eLearning
Mobile Security	FedVTE
Network Access in Microsoft Windows Server 2008	eLearning
Networking Fundamentals	FedVTE
Networking Fundamentals in Linux	eLearning
Octave Allegro	FedVTE
Optimizing a Database Data Recovery Plan for SQL Server 2005	eLearning
Oracle Database 11g	eLearning
Penetration Testing	FedVTE
Perl Language Fundamentals	eLearning
Planning, Implementing and Maintaining User, Computer, and Group Policies and Strategies	eLearning
PSTN and VoIP Fundamentals	eLearning
Quality Systems, Models, and Theories	eLearning
RaD-X 101	Classroom
RaD-X 301	Classroom
Risk Management	eLearning
Risk Management Planning (PMBOK® Guide Fifth Edition)	eLearning
Risk Response, Monitor, and Control	eLearning

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Training Course Name	Method of Delivery
SCCP	eLearning
Securing Firewalls and ACLs	Classroom
Securing the IT Environment	eLearning
Securing Web Applications	Classroom
Securing Windows 2008	Classroom
Securing Windows 7	Classroom
Securing Windows XP	Classroom
Securing Wireless Networks	Classroom
Security + Prep	Classroom
Software Engineering	eLearning
Software Program Control Flow Fundamentals	eLearning
Software Test Management	eLearning
SQL Server 2008 R2	eLearning
SRR UNIX	Classroom
SRR Walk-Through for Networks	Classroom
SRR Windows	Classroom
SSCP Domain: Networks and Telecommunications	eLearning
Starting to Program with Perl	eLearning
Static Techniques and Test Design in Software Testing	eLearning
Statistics and Probability in Six Sigma	eLearning
Strategic Approaches to Risk Management	eLearning
Supply Chain Awareness	FedVTE
System Exploits and Intrusion Detection	Classroom

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Training Course Name	Method of Delivery
Testing Throughout the Software Life Cycle	eLearning
Tool Support in Software Testing	eLearning
Traditional & Physical Security – Principles and Practices	Classroom
UNIX and Linux Security	Classroom
UNIX Fundamentals	eLearning
UNIX Fundamentals	eLearning
UNIX Security for Systems Administrators	Classroom
US-CERT™ Network Analyst	FedVTE
Using LINQ and XML with ADO.NET4 and Visual Basic	eLearning
Using PKI	IASE Website
VMS	FedVTE
VMware vSphere 5	eLearning
VoIP Quality and Security	eLearning
VoIP Technologies	eLearning
Web Development Fundamentals	eLearning
White-Box Software Testing Techniques	eLearning
Windows Application Development with Visual Basic 2010	eLearning
Windows PowerShell 2.0	Classroom
Windows Server 2003 IP&R: Part 1	IASE Website
Windows Server 2003 IP&R: Part 2	IASE Website
Working with the ADO.NET Entity Framework 4 using C# 2010	eLearning
Working with the ADO.NET Entity	eLearning

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**  
**SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Training Course Name	Method of Delivery
Framework 4 using Visual Basic 2010	

DRAFT



## APPENDIX D – TRAINING RESOURCES

### Training Resources

#### IASE Website

- a. Web-based training <http://iase.disa.mil/eta/online-catalog.html>
- b. Classroom training <http://powhatan.iiie.disa.mil>

#### FedVTE Website

- a. <https://www.fedvte-fsi.gov/>

#### CMIS IT Training Catalog

- a. <https://cmis.disa.mil/training/iatraining/iatraining.cfm>

#### Courses per Proficiency Level

Courses are subject to regular changes. The most current listing of courses can be found at:

- a. [https://powhatan.iiie.disa.mil/specialty\\_courses/](https://powhatan.iiie.disa.mil/specialty_courses/)

## APPENDIX E – SUPPORT AND POC LIST

### **Support**

If you are seeking technical support ...

### **Web Resources**

#### *Official Website*

(NIPRNet) <http://www.disa.mil/>

(SIPRNet) <http://www.disa.smil.mil/>

DRAFT

**APPENDIX F - ACRONYM LIST**

The list of Acronyms is provided for the convenience of the reader and is intended to reflect those acronyms used in the base document. As the document evolves and changes, every effort will be taken to keep it current and consistent within DoD standards.

**Table F-1: Acronym List**

Acronym	Definition
ACAS	Assured Compliance Assessment Solution
AIS	Automated Information System
AMD	Advanced Micro Devices
AoA	Analysis of Alternatives
AOR	Area of Responsibility
ATO	Authorization to Operate
AV	Architectural Viewpoint
BCP	Business Continuity Plan
BIOS	Basic Input/Output System
BPMN	Business Process Modeling Notation
BSM	Business Systems Modernization
C&A	Certification and Accreditation
CA	Certifying Authority
CAPE	Cost Assessment and Program Evaluation
CC	Common Criteria
CDR	Critical Design Review
CCEV	Common Criteria Evaluation and Validation Scheme
CCM	Configuration and Control Management
CCRA	Common Criteria Recognition Arrangement
CCSD	Command Communication Service Designator
CEM	Common Methodology for Information Technology Security Evaluation
CI	Configuration Item
CIO	Chief Information Officer

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Acronym	Definition
CM	Configuration Management
CMIS	Corporate Management Information System
CMVP	Cryptomodule Validation Program
COI	Communities of Interest
CONOPS	Concept of Operations
COTS	Commercial off-the-shelf
CPU	Central Processing Unit
CSMA/CD	Carrier Sense Multiple Access Collision Detection
CUI	Controlled Unclassified Information
CWDP	Cyber Work Role Development Plan
CWID	Coalition Warrior Interoperability Demonstration
DAA	Designated Accrediting Authority
DAG	Defense Acquisition Guide
DARS	Department of Defense Architecture Registry System
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DLL	Dynamic-Link Library
DM2	Department of Defense Architecture Framework Meta-Model
DMR	Department of Defense Meta Data Registry
DNSSEC	Domain Name System Security Extension
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DODIN	Department of Defense Information Networks
DoD EA BRM	Department of Defense Enterprise Architecture Business

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Acronym	Definition
	Reference Model
DoS	Denial of Service
EA	Enterprise Architecture
EAL	Evaluation Assurance Level
eMASS	Enterprise Mission Assurance Support Service
EMD	Engineering and Manufacturing Development
EVM	Earned Value Management
FBCA	Federal Bridge Certificate Authority (FBCA)
FCI	File Classification Infrastructure
FedVTE	Federal Virtual Training Environment
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FoS	Family of Systems
FSO	Field Security Operations
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
ICD	Interface Control Document
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IP	Internet Protocol

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Acronym	Definition
IPSec	Internet Protocol Security
IS	Information System
IT	Information Technology
JCIDS	Joint Capabilities Integration and Development System
JCT&CS	Joint Cyberspace Training and Certifications Standards
JFCOM	U.S. Joint Forces Command
KPP	Key Performance Parameters
KSA	Knowledge, Skills, and Abilities
KSA	Key System Attributes
LAN	Local Area Network
MA	Mission Area
MAC	Mission Assurance Category
MDAP	Major Defense Acquisition Program
MOA	Memorandum-of-Agreement
MODAF	Ministry of Defense Architecture Framework
MTBF	Mean Time Between Failure
MTBSO	Mean Time Between Service Outage
MTTR	Mean Time to Repair
NAF	North Atlantic Treaty Organization Architecture Framework
NDA	Non Disclosure Agreement
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NICE	National Initiative for Cybersecurity Education
NII	Networks & Information Integration
NIST	National Institute of Standards and Technology
ODASD	Office of the Deputy Assistant Secretary of Defense
OMB	Office of Management and Budget
OV	Operational Viewpoint
P&D	Production and Development

**UNCLASSIFIED//FOR OFFICIAL USE ONLY****SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Acronym	Definition
PAA	Principal Accrediting Authority
PDR	Preliminary Design Review
PES	Physical Exchange Specifications
PKE	Public Key Enabled
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POC	Point of Contact
PM	Program Manager
PMO	Project Management Office
PP	Protection Profiles
QS	Qualification Standard
RAM	Random Access Memory
RFP	Request for Proposal
R&M	Reliability and Manageability
RMS	Rights Management Services
SCCVI	Secure Configuration Compliance Validation Initiative
SE	Systems Engineering
SEP	Systems Engineering Plan
SFR	System Functional Review
SIP	System Identification Profile
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SoS	System of Systems
SRA	Schedule Risk Assessment
TAG	Technical Advisory Group
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TD	Technology Development
TOGAF	The Open Group Architecture Framework

**UNCLASSIFIED//FOR OFFICIAL USE ONLY**  
**SYSTEMS ARCHITECT PROCEDURE GUIDE V0 R1**

---

Acronym	Definition
TPM	Technical Performance Measures
UPS	Uninterruptible Power Supplies
VMS	Vulnerability Management System
V&V	Verification and Validation
WAN	Wide Area Network
WBS	Work Breakdown Structure
WG	Working Group



