

Version <X.Y>

<Date>

Prepared for:

<Organization>

Prepared by:

<Author(s)>

Contract: <Contract ID>

<Other Front Matter>

<Organization-specific legal boilerplate, if applicable>

For Internal <Organization> Use. This document was prepared for authorized distribution only. It has not been approved for public release.



This document is derived from  
*MITRE Adaptive Capabilities Testing (ACT)™*.  
act.mitre.org | act@mitre.org

<Organization>

MITRE Adaptive Capabilities Testing (ACT)™

Authorization Boundary Diagram (ABD) Guidance

Record of Changes

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Responsible Author | Description of Change |
| 1.0 | May 30, 2025 | Nate Lee Andrew Bennett Ernie Riviere Jim Bielski | Initial release of MITRE ACT templates and work aids. |

**Note to the Author Using this Template:**

This is a *template* for producing a MITRE ACT template tailored to your specific organization. Everything in this template can and should be customized by you to meet your organization’s specific needs and objectives.

Various objects and sections of text throughout the template are highlighted – these are **items that are very likely to require customization**, but you are free and encouraged to **edit the entire document and process** to suit your organization’s needs. By documenting your actual ACT process (including how it deviates from the baseline herein) in this template you are ensuring that your ACT assessments are consistent, repeatable, and can be accurately compared to assessments from other organizations’ implementations of ACT.

Table of Contents

[1. Overview 1](#_Toc199255112)

[2. DoDAF Views vs. ABDs 1](#_Toc199255113)

[2.1 Differences Between DoDAF Views and ABDs 2](#_Toc199255114)

[2.2 Similarities Between Operational and System Views 3](#_Toc199255115)

[3. Authorization Boundary Diagram 3](#_Toc199255116)

[3.1 Example Diagram 4](#_Toc199255117)

[3.2 Standards 4](#_Toc199255118)

[3.3 Elements 5](#_Toc199255119)

[3.3.1 Labels and Lends 5](#_Toc199255120)

[3.3.2 Network Components 5](#_Toc199255121)

[3.3.3 Cloud Integration 5](#_Toc199255122)

[3.3.4 Security Zones 6](#_Toc199255123)

[3.3.5 Connection and Communication Paths 6](#_Toc199255124)

[3.3.6 Security Controls 6](#_Toc199255125)

[3.3.7 Asset Identification 6](#_Toc199255126)

[3.3.8 Boundaries 6](#_Toc199255127)

[3.4 Optional Information 6](#_Toc199255128)

[3.4.1 Data Flow 7](#_Toc199255129)

[3.4.2 Monitoring and Logging 7](#_Toc199255130)

[3.4.3 Backup and Recovery Systems 7](#_Toc199255131)

[3.4.4 Administrative Interfaces 7](#_Toc199255132)

[3.5 Generation and Update 7](#_Toc199255133)

# 

# Overview

This document provides guidance for creating Authorization Boundary Diagrams (ABDs) that meet the intent of the National Institute of Standards and Technology (NIST) / Department of Defense (DoD) Risk Management Framework (RMF). NIST Special Publication (SP) 800-53 Revision 5 states that the Authorization Boundary[[1]](#footnote-2) encompasses “all components of an information system to be authorized for operation by an authorizing official.” This excludes separately authorized systems to which the information system is connected.

ABDs are critical elements of system security documentation (such as the System Security Plan (SSP)) and system assessment documentation (such as a Security Assessment Report (SAR) or Risk Assessment Report (RAR)) and are required for inclusion in Authorization to Connect (ATC) or Authorization to Operate (ATO) packages. These diagrams visually document the system architecture, providing clarity regarding components within the scope of authorization boundary. Additionally, ABDs play a vital role in risk management by preventing scope creep and ensuring all components within the boundary are subject to appropriate security controls.

This document outlines the necessary elements for constructing an ABD which might include network components, security zones, connection paths, security controls, asset identification, and boundaries. Optional information (such as data flow, monitoring and logging, backup and recovery systems, and administrative interfaces), is also discussed to enhance the utility of the diagrams for Authorizing Officials (AOs).

This document emphasizes considerations for generating ABDs, including defining trust boundaries, documenting interconnections with other authorized systems, marking data flows, and ensuring legibility and consistency with system documentation. Best practices for diagram generation, including the use of standardized symbols and regular updates to reflect network changes, are also highlighted.

By adhering to the guidance provided in this document, stakeholders can create clear, actionable, and accurate ABDs that support ATC/ATO activities, compliance, risk mitigation, and effective communication across all relevant parties.

# DoDAF Views vs. ABDs

**Note to the Author:** This Section is intended to help those familiar with DoD RMF and DoDAF to understand the difference between ABDs and the diagrams required by DoDAF. If this situation is not applicable to your organization, you might wish to remove this Section entirely.

The Department of Defense Architecture Framework (DoDAF)[[2]](#footnote-3) is a standardized framework used by the U.S. Department of Defense (DoD) to develop, organize, and present architecture descriptions for systems and processes. DoDAF organizes architectural information into Views that address different aspects of a system or enterprise, and two of these views are often confused with the ABD:

* **Operational Viewpoint (OV)** – provides the "what" and "why" of the mission: tasks, activities, and information exchanges.
* **Systems Viewpoint (SV)** – provides the "how" in terms of system implementation: systems, interconnections, and performance.

The OV and SV are closely linked, as the operational requirements defined in the OV drive the technical solutions described in the SV. Together, they ensure that the architecture aligns operational needs with technical capabilities.

ABDs **ARE NOT** the same as the DoDAF OV or SV:

**DoDAF OV/SV** helps implementors ensure that technical capabilities are aligned with mission needs, enabling stakeholders to design, analyze, and implement systems that effectively support operational objectives.

**NIST ABD** helps assessors and authorizing officials draw a clear security boundary around those systems to support risk-based authorization.

## Differences Between DoDAF Views and ABDs

Table : Differences Between OV, SV, and ABD

|  |  |  |  |
| --- | --- | --- | --- |
|  | DoDAF Operational View (OV) | DoDAF System View (SV) | NIST Authorization Boundary Diagram (ABD) |
| Purpose | **Purpose**: Provides a high-level perspective on how the system or enterprise operates in its intended environment. It emphasizes the relationships between operational elements, such as organizations, roles, and workflows, without delving into the technical implementation details. | **Purpose:** Defines the systems, technologies, and resources that support the operational needs described in the OV. The SV bridges the gap between operational requirements and technical solutions. It describes the architecture of the systems, their functionality, interconnections, and how they support the operational activities. | **Purpose**: Visually shows the scope of a system or set of systems included within a security control implementation, risk assessment, Authority to Connect (ATC)/Authorization to Operate (ATO) |
| Audience | Architects, systems engineers, acquisition officials, planners. | | Security assessors, authorizing officials, system owners, compliance teams. |
| Use Case | Enterprise-level planning and capability alignment. | | Security compliance, ATO/ATC preparation, RMF documentation. |
|  | **Products from Views & Diagrams** | | |
| **OV-1**: High-level graphical view of the operational concept (mission overview). | **SV-1**: Systems Interface Description (shows system nodes and their interconnections). | **Diagram:** Visual representation of network with a demarcation of “What is in Scope”. |
| **OV-2**: Operational Node Connectivity Description (shows relationships between operational nodes). | **SV-2**: Systems Communication Description (details system-level communications). | **Additional Diagrams**: in the situation where there is too much information to put in a single diagram, multiple diagrams are common. |
| **OV-5**: Operational Activity Model (details the activities performed and their relationships). | **SV-4**: Systems Functionality Description (describes system functions and their relationships). |
| **OV-6**: Operational Rules Model (defines constraints and rules governing operations). | **SV-6**: Systems Data Exchange Matrix (defines data exchanges between systems). |

## Similarities Between Operational and System Views

DoDAF and ABDs both require a deep understanding of system dependencies to be useful for their intended audiences. All three share many similar aspects as shown by the table below:

Table . Similarities Between OV, SV, and ABD

|  |  |  |
| --- | --- | --- |
| Similarity | DoDAF OV/SV | NIST Authorization Boundary Diagram (ABD) |
| Defining Boundaries | Operational and system boundaries | System scope for security assessment |
| Interconnections and Interfaces | Relationships between nodes/systems | External connections and dependencies |
| Data Flows | Operational and system data flows | Internal and external data exchanges |
| Risk Management | Managing mission risks | Identifying vulnerabilities and risks |
| Stakeholder Communication | Visual tool for mission understanding | Visual tool for security understanding |
| Documentation and Compliance | Required for DoD architecture | Required for RMF process |
| System Dependencies | Operational and system dependencies | External system dependencies |
| Operational-Technical Alignment | Systems supporting mission needs | Security controls supporting operations |

# Authorization Boundary Diagram

It is critically important for both the System Team and Assessment Teams to understand the Authorization Boundary and to ensure that they are clearly and unambiguously defined in system security documentation (such as the SSP) and testing documentation (such as the SAR). **The ABD visually defines which components of the architecture are part of the authorized system (and thus are the responsibility of the system personnel).** Put another way, **the ABD helps the reader clearly understand which components are “in scope” and which are “out of scope” for assessment.** Some systems might require multiple ABDs in order to provide the appropriate level of detail.

## Example Diagram

The example ABD below represents an "Example Test System" (TST) that is referenced throughout the ACT Guidance, Documentation, and Templates to illustrate key ACT concepts. In this example, the authorization boundary is outlined by the green dashed box.

The authorization boundary is separate and distinct from the “assessment boundary”, which is *not* shown in the example. While the *authorization* boundary indicates the full set of components that comprise the authorized system, the *assessment* boundary indicates which subset (up-to and potentially including the full set) of system components will be assessed. The assessment boundary would be defined in a separate “Assessment Boundary Diagram”.

Diagram

AI-generated content may be incorrect.

Figure 1. Example Authorization Boundary Diagram

## Standards

Good Authorization Boundary Diagrams:

1. Clearly define the Authorization Boundary with a **predominant border**, defined in the legend, drawn around all system components and services included. The boundary might comprise a single shape or multiple separate shapes.
2. Document interconnections with other authorized systems (*i.e.*, other Authorization Boundaries).
   1. Identify any connections to other systems/networks/enclaves, including:
      1. The name of the organization that owns the system/network/enclave, as appropriate.
      2. The connection type (e.g., wireless, dedicated point-to-point, etc.), as appropriate.
      3. The organization type (e.g., Federal agency, contractor, etc.), as appropriate.
      4. Data flows clearly marked as unidirectional or bi-directional.
      5. Protocols, ports, etc. in use by the system should be depicted as appropriate.
   2. Note that sometimes components are notionally within the authorization boundary of the system but are actually part of / provided by one or more separate authorized systems.
3. Clearly legible in the provided format (e.g., no “pixelization”), and all labels and titles are easy to read.
4. Provide a last-updated date and legend.
5. Identify equipment/component inventory consistent with documented hardware and software inventories (including firewalls, Intrusion Detection or Prevention Systems (IDS/IPS), routers, switches, Internet Protocol (IP) addresses, encryption devices, etc.).
6. Identify all cybersecurity or cybersecurity-enabled products deployed within the authorization boundary.
7. Use formal names for all components, ensuring that names match system documentation (i.e, functional specifications, configuration guides, SSP, etc.).

## Elements

ABDs typically include the following:

### Labels and Lends

* Symbols used for devices, connections, and security controls.
* Color coding for different zones or data types.

### Network Components

* **Endpoints**: Workstations, laptops, mobile devices, servers, etc.
* **Network Devices**: Routers, switches, firewalls, load balancers, etc.
* **Storage Systems**: Databases, file servers, cloud storage, etc.
* **Virtualized Components**: Virtual machines, containers, hypervisors, etc.
* **IoT Devices**: Sensors, cameras, smart devices, etc.

### Cloud Integration

For hybrid or cloud environments, include:

* **Cloud Service Providers**: AWS, Azure, Google Cloud, etc.
* **Cloud Security Controls**: Identity and access management (IAM), cloud firewalls, etc.
* **Data Transfer Points**: Connections between on-premises and cloud systems.

### Security Zones

* **Logical Segmentation:** Show how the network is divided into subnets, VLANs, or zones (e.g., DMZ, internal network, guest network).
* **Physical Segmentation:** Illustrate physical connections between devices, including cabling, wireless access points, and physical switches.

### Connection and Communication Paths

* **Ports & Protocols**: Specify communication protocols (e.g., HTTPS, SSH, FTP, etc.).
* **Encryption**: Indicate encrypted communication paths (e.g., VPN tunnels, TLS/SSL).
* **External Connections**: Show connections to external networks, such as the internet, partner networks, or cloud services.

### Security Controls

* **Firewalls**: Network firewalls, web application firewalls (WAFs), etc.
* **Intrusion Detection/Prevention Systems (IDS/IPS):** monitoring and blocking malicious traffic.
* **Access Control Mechanisms:** Authentication servers, role-based access control (RBAC), etc.
* **Endpoint Protection:** Antivirus, endpoint detection and response (EDR) solutions.
* **Encryption Tools:** VPNs, TLS/SSL, and other encryption mechanisms.

### Asset Identification

Unique identifiers should be indicated (as appropriate) for each item in the diagram, such as:

* **Hostnames**
* **IP addresses**
* **MAC addresses**
* **Asset tags or inventory numbers**

### Boundaries

Clearly mark trust boundaries where different levels of security apply. For example:

* Boundary between internal network and DMZ.
* Boundary between on-premises systems and cloud services.

## Optional Information

Although the following example Elements are not strictly required, they are often helpful to the Authorizing Official (AO).

### Data Flow

Illustrate how data flows through the network:

* **Inbound and Outbound Traffic**: Indicate traffic entering and leaving the network.
* **Internal Traffic**: Show how data moves between systems within the network.
* **Sensitive Data Paths**: Highlight paths where sensitive or regulated data is transmitted.

### Monitoring and Logging

* **SIEM Systems**: Security Information and Event Management tools.
* **Log Servers**: Centralized logging systems.
* **Network Monitoring Tools**: Tools for real-time traffic analysis.

### Backup and Recovery Systems

* **Backup Servers**: On-premises or cloud-based.
* **Replication Paths**: For data redundancy.
* **Disaster Recovery Sites**: Secondary data centers or cloud recovery systems.

### Administrative Interfaces

Indicate administrative interfaces and their security:

* **Management Consoles**: For network devices, servers, and cloud services.
* **Secure Access Methods**: VPNs, bastion hosts, or jump servers.

## Generation and Update

The ABD often originates from a network diagram that outlines components, devices, and connections within the system; however, additional technical details are usually required to develop an adequate boundary diagram. These details can usually be obtained from readily available sources:

* **Design documents** often contain various architecture and functional views that can aid in understanding the system components, component connections, and interconnections with external systems.
* **Network monitoring tools** are often capable of providing real-time hardware and software mappings of the current network infrastructure.
* **Security Information and Event Management (SIEM) solutions** often facilitate the collection and aggregation of component and connection data.
* **Software and Hardware inventories** should contain comprehensive lists of the software and hardware components comprising the system.
* **Assessment Plans** from past assessments should containassessment team understandings of the authorization boundary at that time.

**The diagram should be regularly updated** to reflect changes in the deployment, configuration, components, functions, and environment. Standardized symbols (aligned with industry conventions for representing network components) should be used to ensure consistency, accuracy, and future understandability.

1. NIST Special Publication 800-37 Revision 2 states “*Historically, NIST has used the terms Authorization Boundary, System Boundary, and Accreditation Boundary interchangeably. In the interest of clarity, accuracy, and use of standardized terminology, the term Authorization Boundary is now used exclusively by NIST to refer to the set of system elements comprising the system to be authorized for operation or authorized for use by an Authorizing Official (i.e., the scope of the authorization).”* [↑](#footnote-ref-2)
2. <https://dodcio.defense.gov/library/dod-architecture-framework/> [↑](#footnote-ref-3)