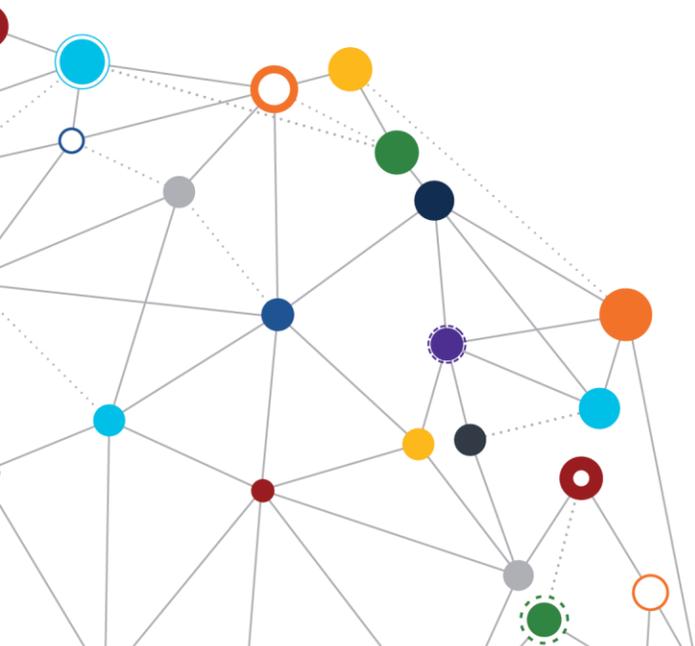


OFFICE OF
INFORMATION
AND TECHNOLOGY

Identity and Access Management (IAM) Enterprise Design Pattern

Risk Assessment

September 2018 | Demand Management Division



VA



U.S. Department of Veterans Affairs
Office of Information and Technology



Table of Contents

- 1 Context 3**
- 2 Challenge 3**
- 3 Guidance..... 4**
 - 3.1 Establish IAM Assurance Levels 5
- 4 Application of Practices 6**
 - 4.1 Migration of Electronic Health Record (EHR) Solution 6
 - 4.1.1 Purpose 6
 - 4.1.2 Assumptions..... 6
 - 4.1.3 Use Case Description 7
 - 4.2 Key Practices 7
- 5 Impacts 8**
- Appendix A: Acceptable AL Combinations Example 9**
- Appendix B: References 10**

- Figure 1: Overview of IAM Future Progression..... 4
- Figure 2: IAM Risk Process Overview..... 5

- Table 1: Change Matrix..... 2
- Table 2 : Key Practices IAM Risk Assessment EDP 7

Table 1: Change Matrix

Version	Date	Description of Updates
1.0	9/20/18	IAM EDP Risk Assessment Segment document approved



1 Context

The Department of Veterans Affairs (VA) has a unified enterprise Identity and Access Management (IAM) program to coordinate secure access to VA resources for both internal and external users. IAM services are guided by the Office of Management and Budget (OMB) M 11-11, the Federal Information Processing Standard (FIPS) 200, the National Institute of Standards and Technology (NIST) guidelines (800-63 and 800-53 per Appendix D), and the Federal Identity, Credential, and Access Management (FICAM) initiative.

VA has two general populations of users who require access: (1) internal users include employees, contractors, trainees, and volunteers, and (2) external users, comprised of Veterans, beneficiaries, and health partners, including employees and contractors from other Government agencies. All require varying levels of access to interact with VA services.

2 Challenge

VA must set the foundation for IAM through proper risk assessment of applications and identification of the IAM-related business requirements, in compliance with NIST 800-63-3. This risk assessment will drive the requirements for identity proofing, provisioning, authentication, federation, and technologies supporting IAM capabilities. Figure 1 shows the progression required from both the user and system owner to gain access to resources using IAM services. The assurance level (AL) guides the requirements for each of these areas. The area addressed in this document is highlighted in red.

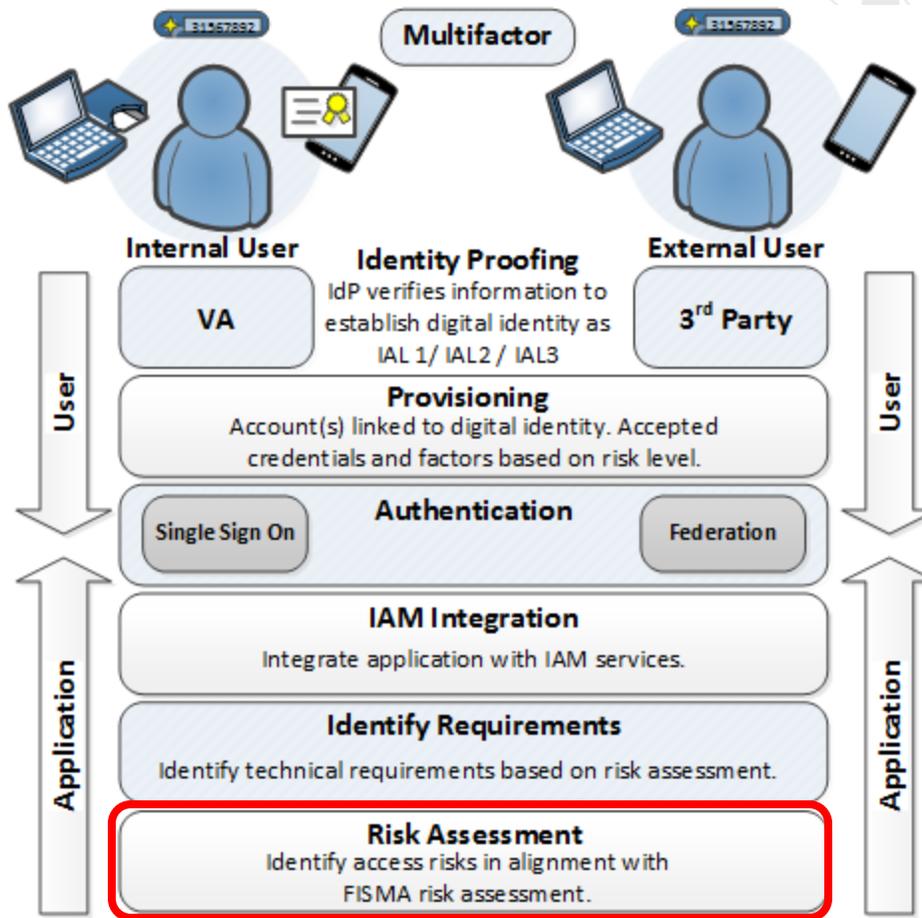


Figure 1: Overview of IAM Future Progression¹

3 Guidance

Projects that go through the VA Veteran-Focused Integration Process (VIP)² are subject to the VA Assessment and Authorization (A&A) Process³ and Risk Management Framework (RMF).⁴

¹ Figure 1 was created by the VA Office of Information and Technology (OIT) Architecture and Engineering Service (AES) Enterprise Design Pattern (EDP) Team from information obtained from VA OIT IAM Subject Matter Experts (SMEs) and the National Institute of Standards and Technology (NIST) Special Publication 800-63A at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.

² The VIP 3.1 Guide, April 2018, can be referenced at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=27>.

³ For additional information on VA Assessment and Authorization, refer to https://www.va.gov/PROPATH/map_library/process_AAA_ext.pdf.

⁴ The NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, provides additional information at <https://pages.nist.gov/800-63-3/sp800-63-3.html>. The VA Handbook 6500, Risk Management Framework for VA Information Systems, can be referenced at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FTYPE=2.

This document provides information on how risk assessments that are performed as part of RMF are used to guide the technical design of IAM solutions.

3.1 Establish IAM Assurance Levels

A risk assessment is used to determine the technical requirements for the different areas of each IAM solution. NIST uses AL to define three (3) basic levels of risk (AL1, AL2, AL3), and defines the requirements separately for Enrollment and Identity Proofing (IAL), Authentication (AAL), and Federation (FAL). NIST 800-63-3 requires that all systems that undergo the RMF process shall perform a separate risk assessment based on the business needs of the service, including the type of access needed and actions performed. As part of the RMF process, the system owner will complete a separate risk assessment of each area: IAL, AAL, and FAL. The potential impacts will follow FIPS 199 and be guided by NIST 800-63-3 to map the potential impact to an AL of 1, 2, or 3 as described in Figure 2. The previous method of using four LOAs as a single ordinal across all areas of IAM has been retired. Now each area is assigned its own AL. While these levels may often be the same across each area, this is not required.

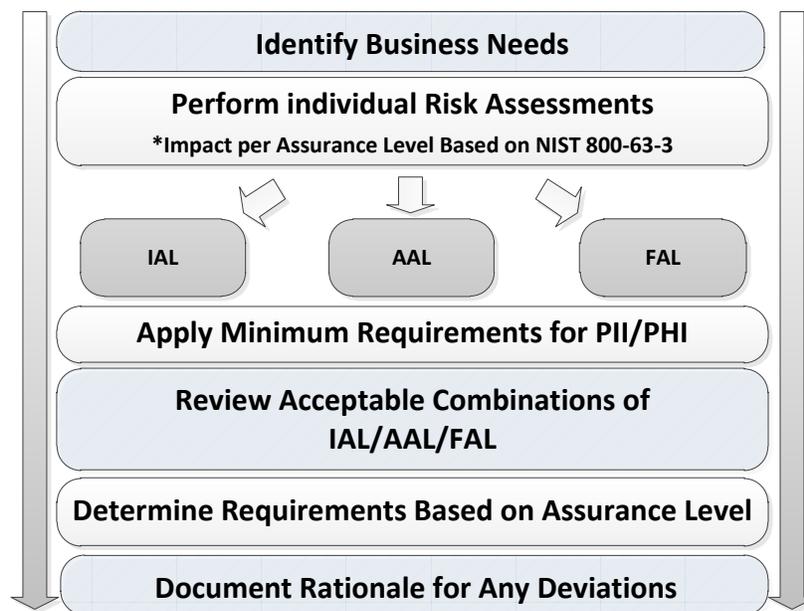


Figure 2: IAM Risk Process Overview

The emphasis is on the flexibility to raise one or more areas, as necessary, to maximize privacy-enhancing techniques at any AL. The focus of the risk assessment is on evaluating risk to the user and data, accessed as part of the digital transaction, and not the entire business process. For example, a job posting site may allow an individual to post a resume. The identity proofing may be IAL1, which allows pseudonymous access, where a user could post a resume on behalf of someone else. However, AAL2 would be required; this is due to the likely inclusion of personal information in the resume and the need to restrict access to the same user. While the business process of hiring an applicant would require a higher level of identity proofing, this

verification may occur later. Here, the risk related to the online transaction of allowing a resume to be submitted to a portal does not have to match the overall risk to the business process.

Once the initial ALs are determined, they will be reviewed, as described by the VA RMF process,⁵ to ensure they meet the minimum requirements for systems accessing personally identifiable information (PII)/Protected Health Information (PHI); and the acceptable combinations of ALs for each area. The AL review confirmations drive the technical requirements for each area. If the assessed AL and the implemented AL differ, this will be documented as an artifact with the supporting rationale. For example, a system granting external access to health records may assess the risk of the unauthorized release of sensitive information as Low Impact to ease the requirements for identity proofing. However, VA policy may require a minimum of Moderate when PHI is accessed. The risk assessment could also result in IAL1, AAL3, and FAL3, but IAL2 may be the lowest combination allowed when FAL3 is used. If the system was assessed at IAL2, based on these conditions, and proceeded to implement IAL1, a rationale would be provided and recorded as an artifact for the system authorization. Figure 2 provides a high-level overview.

4 Application of Practices

The following use case relates to applying the described risk management principles to solution development.

4.1 Migration of Electronic Health Record (EHR) Solution

4.1.1 Purpose

The Veterans Health Administration (VHA) is upgrading to a new solution to allow Veterans to access their EHR. The System Owner wants to determine the technical requirements for IAM service integration.

4.1.2 Assumptions

- The database contains sensitive information, including PHI.
- The EHR legacy solution uses the VA SSOe service.

⁵ Refer to the VA Handbook 6500, Risk Management Framework for VA Information Systems at https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FTYPE=2.

4.1.3 Use Case Description

- The System Owner submits the business case for a new solution as a VIP request (VIPR) to begin the intake process for VIP.
- A risk assessment is required as part of the RMF process to determine the AL and corresponding IAM solution requirements.
- The Authority to Operate (ATO) artifacts are not required until Critical Decision 2 (CD2) in VIP. Therefore, projected ALs must be used before Critical Decision 1 (CD1) to determine if the ALs for IAM services can be met as part of the Analysis of Alternatives (AoA). IAL2/AAL2/FAL2 are projected.
- The ATO process is completed as part of CD2. The risk assessment resulted in IAL3, AAL3 and FAL3 for the solution.
- The draft solution is not compliant with the project's assessed AL.
- IAL 3, AAL3, and FAL3 are recorded for the risk assessment; but IAL2, AAL2, and FAL2 are implemented based on the business justification that the increased security would create a significant barrier to access for many Veterans.
- The artifacts are recorded as part of the ATO, and the SSOe service is implemented to meet compliance.

4.2 Key Practices

Table 2 highlights key practices identified in this EDP.

Table 2 : Key Practices IAM Risk Assessment EDP

Category	Area	Description
Identity and Access Management	Security Categorization	Each IAL, AAL, FAL category shall be evaluated separately and assigned an AL of 1, 2 or 3.
Identity and Access Management	Security Categorization	IAM risk assessments shall assess potential impact to IAL, AAL and FAL, as described in FIPS 199, based on the digital or online process.
Identity and Access Management	Risk Assessment	The risk assessment profile shall be compared to the impact profile associated with each assurance level, as described in NIST 800-63-3.
Identity and Access Management	Risk Assessment	System owners shall follow the Table of Acceptable Combinations of AAL, IAL and FAL

Category	Area	Description
		ALs, created by VA to include minimum requirements for PII/PHI to control risk. ⁶
Identity and Access Management	Risk Assessment	Risk assessment artifacts shall contain: <ul style="list-style-type: none"> • The Assessed AL • The Implemented AL • A rationale, if the assessed level differs from implementation level, along with compensating controls.
Identity and Access Management	Security Controls	System owners shall use the ALs defined through the RMF process to select controls or enterprise services that can meet the required controls.

5 Impacts

If risk management is not used to define technical requirements for IAM components of VA solutions, the following risks are increased:

- FISMA non-compliance, contributing to a material weakness or other audit findings by external agencies with oversight
- Inadequate technical protections for sensitive data that may contribute to unauthorized access or data breach

⁶ Executive Order 13681 requires the use of multifactor (MFA) for any access to personal data (not limited to financial transactions). <https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions>

Appendix A: Acceptable AL Combinations Example

The table below provides an example of how acceptable combinations of ALs may be documented. This is for illustrative purposes only.

Category	IAL1	IAL2	IAL3	AAL1	AAL2	AAL3	FAL1	FAL2	FAL3
No PII/PHI	Yes								
PII/PHI	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes
Prescriptions/Financial	No	No	Yes	No	No	Yes	No	No	Yes
IAL1	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes	Yes
IAL2	N/A	N/A	N/A	No	Yes	Yes	No	Yes	Yes
IAL3	N/A	N/A	N/A	No	Yes	Yes	No	No	Yes
AAL1	Yes	No	No	N/A	N/A	N/A	Yes	No	No
AAL2	Yes	Yes	Yes	N/A	N/A	N/A	Yes	Yes	No
AAL3	Yes	Yes	Yes	N/A	N/A	N/A	Yes	Yes	Yes

Appendix B: References

- DEA User Stories:
<https://vaww.portal2.va.gov/sites/asd/TechStrat/IPTS/SitePages/Home.aspx>
- FISMA User Stories:
<https://vaww.portal2.va.gov/sites/asd/AERB/FISMA Security Compliance/SitePages/Home.aspx>
- TRM: <http://trm.oit.va.gov/>
- NIST 800-63-3: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>
- VA 6500.3: http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=733&FType=2
- VA 6510 (under revision):
http://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=823&FType=2

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.

Statement of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and shall not be used for advertising or product endorsement purposes.