Introduction
Cloud Identity Playbook
Digital Accessibility Playbook
Digital Identity Risk Assessment Playbook
Step 1. Identify Users, Transactions, and Roles
Step 2. Identify Risks and Assurance Levels
Step 3. Determine Steps to Meet Assurance
Step 4. Finalize Digital Identity Acceptance Statement
Step 5. Monitor Changes
Step 6. Reassess
Step 7. Reconsider PIA
Step 8. Update
Step 9. Continue Risk Management
Step 10. Reassess
Step 11. Reconsider PIA
Step 12. Update
Step 13. Continue Risk Management
Step 14. Reassess
Step 15. Reconsider PIA
Step 16. Update
Step 17. Continue Risk Management
Digital Signature Implementation Playbook
Digital Signature Policy Playbook
Cross-Agency Identity Playbook
Enterprise Single Sign-On Playbook
Phishing-Resistant Authentication Playbook
ICAM Governance Framework Version 2.0
Identity Lifecycle Management Playbook
Privileged Identity Playbook

Digital Identity Risk Assessment Playbook

Date: December 20, 2022 - Version 1.2

Acknowledgments

This playbook reflects the contributions of the Digital Identity Risk Assessment Working group of the Identity, Credential, and Access Management Subcommittee (ICAMSC). The working group was co-chaired by representatives from the General Services Administration and the Department of Homeland Security. Contributions were made by representatives from the Administrative Office of the United States Courts, Center of Medicare and Medicaid Services, Department of Defense (DoD), Department of Energy, Department of Health and Human Services, Department of Justice (DOJ), Department of Labor (DOL), Department of the Treasury (DOT), Department of Transportation (DOT), and General Services Administration (GSA).

Introduction

Digital services rely increasingly on remote engagement as an online transaction. However, an individual's real-life identity may not be known when used to access a digital service.[1] Identity proofing helps organizations establish confidence in the identity of a remote user. Organizations implement identity proofing processes that include the individual connecting the application to the same individual who previously accessed the service. This playbook is intended to apply the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Digital Identity Guidelines, to assist agencies in conducting an Office of Digital Identity Risk Assessment (DIRA) to determine the appropriate identity, authentication, or federation level outlined to access an application.

Purpose

Rare federal agencies offer services through a system of system, such as a website, to their employees, other agencies, and the public. To execute an application, users may need to provide information to establish an account, and log in. These actions are part of the digital identity and authentication process.

DIRAs determine the assurance level for the digital transactions that involve digital identity or authentication. This playbook provides a DIRA process that aligns with NIST SP 800-63-3 Digital Identity guidelines and authentication standards. Key activities in the digital transaction are the user and agency data linked with the applications.

The Digital Identity Risk Assessment playbook helps federal agency Chief Information Officer (CIO) and Chief Information Security Officers (CISO) teams and business application owners to:

- Update and maintain consistent processes,
- Determine whether an agency application requires a DIRA,
- Identify and document business application requirements, DIRA processes, and
- Level and plan to implement DIRA processes.

NIST publishes implementation guides[2] and frequently updated questions (FAQs)[3] for agencies and service providers to use to create information technology systems to meet these standards. This playbook provides consistency, effectiveness, and efficiency in your agency's processes.

How to Use This Playbook

This playbook provides a DIRA process that includes:

- High-Level DIRA Process: A step-by-step guide on how to approach a DIRA process for each agency.
- Agency Templates: Six steps to create efficient and consistent processes. For example, Step 1 includes a template a technical decision tree for a biomedical DIRA for some agencies.
- Appendices: Examples diagrams and templates, and references to policies and standards to use in your agency's processes.

Scope

The DIRA playbook applies to all Federal Information Technology (IT) systems and applications that require identity proofing and authentication.[4] This playbook complements the following standard and policies:

- NIST Special Publication 800-63-3 Digital Identity Guidelines
- Office of Management and Budget Memorandum (OMB) M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management [5]

DIRAs are a component of a risk management process. This playbook complements the use of the Risk Management Framework (RMF) and Federal Information Technology Acquisition Reform Act (FITARA) processes. Business owners and information security officers produce a Digital Identity Risk Assessment (DIRA) to determine the appropriate identity, authentication, or federation level for a digital system or application that is a part of the assessment process.

This playbook does not apply to:

- Non-persons entities[6] such as devices, Internet of Things (IoT), or Machine Learning,
- Facility access,
- Federal Assurance Level 3 solutions,[7] or
- National security systems (NSS).[8]

The following key process terms in this DIRA process and provide plays to help you implement efficiency into your agency's processes.

High-Level DIRA Process

The DIRA process begins with a new application or system is identified or a time-driven or event-driven reassessment is triggered. Once it is determined that a DIRA is needed, application data is collected, and the business owner and information security officer conduct and produce a Digital Identity Risk Assessment (DIRA), as shown in Figure 1.

Figure 1. Example DIRA Process

A high-level DIRA process includes five steps:

1. Identify Users, Transactions, and Roles
2. Identify Risks and Assurance Levels
3. Determine Steps to Meet Assurance
4. Finalize Digital Identity Assessment Statement
5. Reassess

Step 1. Identify Users, Transactions, and Roles

The first step is to identify the users and transaction information as well as the functional and technical roles of the application. There are many addressing in a large assessment scope within the Federal government, such as:

- User Types: Organizational and Non-Organizational users
- Communities of Interest: Employees, Partners, and Public users
- Contract Roles: General, Functional Privileged, and IT Privileged users

These definitions simplify complex requirements related to individuals and privacy information security, and identity and access management concepts.

First, identify the user types and communities of users the application supports. Identifying an application's community of users is important to the DIRA process as communities have different requirements and risk tolerances. Table 1 identifies examples of risk assessments. Table 1 identifies user groups as the non-exhaustive examples of communities.

Table 1. Examples of User Types and Communities

User Type	Description	Examples of Community of Interest
Organizational	An employee or individual the organization desires to have equivalent status of employee	General agency employee users, including employees and direct support contractors
		Other federal government agency users
Non-organizational	All users other than organizational users (i.e., the general public or guests)	U.S., state, local, and tribal agency users
		Non-profit, business, or commercial users
		Public or other users

A transaction[9] is:

> a discrete event between a user and a system that supports a business or programmatic purpose. A government agency may be engaged in business with citizens, businesses, and other agencies, which may involve exchanges of information or the conduct of a financial transaction that involves money.

Application owners and the information security team collaborate to identify, analyze, and assess the digital transactions of the application. Examples of transactions and transaction types are phrased as actions or verbs: Create, Read, Modify, Delete.

> **Key Point**
> Systematic transactions by each community of users for risk assessments. Each community of users may have different transactions depending on the type of data being accessed and what they can use with the data.

Finally, map the community of users to the common roles. Most applications have several different roles and privileges. Table 2 shows a sample. Examples of common user roles include:

- **Guested users**
- Can access information resources provided by the application
- Examples: Employees, general public
- **Functional privileged users**
- Can access information resources provided by the application, and approval workflows
- Examples: Managers
- **Information Technology (IT) privileged users**
- Can access IT systems with read, write, or change access
- Examples: System administrators, security analysts

Table 2 provides examples of user types, transactions, and roles.

Table 2. Examples of User Types and Transactions

User Type	Community of Interest	Example
Organizational	Other federal government agency	Agency employee or contractor User Type1 accesses and uploads document to cross agency collaboration platform (Transaction)
Organizational	Internal agency enterprise user	Agency employee administrator (Role) adds user (Transaction) to agency collaboration platform (Transaction)
Organizational	Internal agency enterprise user	Agency employee or contractor User Type1 accesses and uploads document to outside of the system (Transaction)
Organizational	Internal agency enterprise user	Agency employee supervisor (Role) approves a pending payment (Transaction)
Organizational	Internal agency enterprise user	Agency employee supervisor (Role) processes a payment (Transaction)
Non-organizational	Public user	Public User Type1 searches for national park information and resources (Transaction)
Non-organizational	Public user	Public user User Type1 applies for federal government employment (Transaction)
Non-organizational	Public user	Public user User Type1 retrieves tax information (personally identifiable information [PII]) (Transaction)

Step 2. Identify Risks and Assurance Levels

Determine the digital identity risk for each assurance category by assessing the impacts for each community of user, user type, scenarios, role, and transaction identified in Step 1.

- **Identity Assurance Levels (IAL)** indicate the level of confidence in a claimed identity.
- **Authentication Assurance Levels (AAL)** indicate authentication requirements.
- **Federation Assurance Levels (FAL)** indicate the level of confidence in an assertion that a subscriber's identity is authenticated to a relying party or identity provider application or access system.

The risks and impact assessment considers the risks to both the agency and the user for transactions. The risks can be significant within an organizational impacting the other at all. It's common for government applications to have different assurance levels based on differing impacts to the user and to the agency's mission and operations.

> **Key Point**
> Assurance categories and definitions used in the DIRA process are the same used to determine the overall application system categorization with respects to confidentiality, integrity, and availability (a FIPS 199 assessment).
>
> *However, your overall application system categorization (FIPS 199) is often different than the risks and impacts for the identity and authentication assurance levels for communities of users and transactions in the DIRA.*

Table 3 lists the six impact categories to use. This table is a guideline for categorizing the risks and impacts inherent in your application users and transactions.

Table 3. Impact Definitions

Impact Category	Low	Moderate	High
Inconvenience, distress, or damage to standing or reputation	At worst, limited, short-term inconvenience, distress, or damage to standing or reputation of any party	At worst, serious short-term or limited long-term inconvenience, distress, or damage to standing or reputation of any party	Severe or serious long-term inconvenience, distress, or damage to the standing or reputation of any party. This is authority-sensitive information that could have particularly severe effects or attract adverse attention to the individuals involved
Financial loss or agency liability	At worst, an insignificant or inconsequential financial loss to any party or a minor agency liability requiring settlement	At worst, a serious financial loss to any party or a serious agency liability	Severe or catastrophic financial loss to any party, or severe or catastrophic agency liability
Harm to agency assets or public interests	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are mission capability degradation to the extent and duration that the organization is able to perform its primary functions, but the effectiveness of functions is noticeably reduced	At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are significant degradation in mission capabilities to the extent and duration that the organization is able to perform its primary functions, but the effectiveness of functions is significantly reduced	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic adverse effects are significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness, or a major damage to organizational assets or public interests
Unauthorized release of sensitive information	At worst, a release of personal, U.S. government commercially sensitive information or sensitive information pertaining to a law enforcement investigation with or low impact as defined in FIPS 199	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information or sensitive information pertaining to a law enforcement investigation with a moderate impact as defined in FIPS 199	A release of personal, U.S. government sensitive, or commercially sensitive information or unauthorized release of sensitive information with a high impact as defined in FIPS 199
Personal safety	At worst, minor injury not requiring medical treatment	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment	A risk of serious injury or death
Civil or criminal violations	At worst, a civil or criminal violation of a nature that would not ordinarily be referred to law enforcement offices	At worst, a risk of civil or criminal violations of a nature that would be referred to law enforcement offices	A risk of civil or criminal violations that are of regional importance or international importance

Identity Assurance

Identity Assurance Levels define the processes and solutions used to identify proof users attempting to access a service. Identity proofing establishes confidence in the identity. This contingent requires providing a benefit or information to the wrong user.

- Identity Assurance is "Are you who you say you are?"
- Impacts are "What are the risks to the government or to a user if you are not?"

Defining the IALs for each community of users and transactions from Step 1 is one of the more challenging aspects of the DIRA process. The IAL assessment is a "cross-much-you-can-steal" in collaborate with identity and access management (ICAM) and business owners.

An identity Assurance Level (IAL), the application may or may not require proofing. If an application requires login, a user may only need to provide a user id. Functions under Identity Assurance Level 1 (IAL1) are used to receive notifications. The information may be self-asserted by the user and not verified by the agency. Identity Assurance Level 2 (IAL2) requires the user to provide more personal information about the user ready to be validated and verified. Identity Assurance Level 3 (IAL3) requires an in-person, or live, session, and an address, and of second government issued identity document. Identity Assurance Level 3 (IAL3) requires a biometric and must be verified in person.

> **Key Point**
> The risks and impacts of excessive information collection for identity proofing needs to be strongly considered for each community of users and the transactions.
>
> *For public users and other non-organizational users, privacy benefits and privacy principles are key factors to consider.*
>
> Application owners and agency processes need to include the Senior Agency Official for Privacy to define the risks, impact levels, and the Identity Assurance Levels.

Figure 2 depicts the three Identity Assurance Levels in example terms of the information collected and verified during the identity proofing process.

Figure 2. Identity Assurance Levels

Appendix B: Examples and Templates includes an example of a decision tree of the risk assessment process that defines the Identity Assurance Levels for the community of users and transactions in Step 1.

Authentication Assurance

Authentication Assurance Levels define the strength of the authentication process. Also, it mitigates potential authentication errors (i.e., an attacker accessing a user's account).

- Authentication Assurance is "Are you who you say you are?"
- Impacts are "What are the risks to the government or to a user if you are not?"

Authentication Assurance Levels (AAL) are a single-factor, multi-factor, or multi-factor cryptographic. Authentication Assurance Level 1 (AAL1) at a low risk level requires, including a factor such as a one-time password (OTP) managed by a credential application or a permanent or government mobile phone.[10]

> **Key Point**
> The Risks and Impacts of excessive information collection for identity proofing needs to be strongly considered for each community of users and the transactions.
>
> *For public users and other non-organizational users, privacy benefits and privacy principles are key factors to consider.*
>
> Application owners and agency processes need to include the Senior Agency Official for Privacy to define the risks, impact levels, and the Identity Assurance Levels.

Figure 3 depicts the three Identity Assurance Levels in example terms of the information collected and verified during the identity proofing process.

Figure 3. Authentication Assurance Levels

Appendix B: Examples and Templates includes an example of the risk assessment process flow that defines the Authentication Assurance Levels for the community of users and transactions in Step 1.

Federation Assurance

Federation Assurance Levels (FAL) indicate the assertion protocol used by an application to communicate authentication and attribute information (if applicable) to a relying party (application or access system). This playbook does it recommend a value to the transaction changes or requires a federation assertion.

> **Key Point**
> Federation is an advanced topic with many different assurance and terms.
>
> Use outcome-based assertions and discussions with application owners and business leaders to help identify the FALs.

This playbook explores FALs with the transaction or function before explaining the high level requirements for each assurance.[11] To determine if a per application needs to be used, consider the following questions:

For existing applications and defined users and transactions (Step 1):

- Is the application integrated with any type of agency enterprise single sign-on solution?
- Is the application integrated with an organizational or cross-agency identity provider?
- Are organizational government users and transactions, is the application integrated with an employee's network login?

For new applications and defined users and transactions (Step 1):

- Do the users and users other agency applications and systems need to use cooperation for identity and authentication be assessed?

If your agency's application does not "fit" the set of three assumptions, then the application is "outside" the normal identity and authentication flow. Using the solution definition step (Step 2), and needs a FAL defined for each user community and transaction.

> **Key Point**
> Federation is an advanced topic with many different assurance and terms.
>
> Use outcome-based assertions and discussions with application owners and business leaders to help identify the FALs.

Figure 4 depicts the concept of the three Federation Assurance Levels in example terms.

Figure 4. Federation Assurance Levels

Appendix B: Examples and Templates includes an example of the risk assessment process flow that defines the Federation Assurance Levels for the community of users and transactions in Step 1.

> **Key Point**
> The DIRA provides a minimum level and does not change established credentialing processes. For example, if a DIRA arrive at IAL2, agency leadership may decide to allow a PIV-I credential to be used instead of a PIV-I credential. Or, a PIV-I credentialing process is used.

Step 3. Determine Steps to Meet Assurance Levels

Analyze available technology and solutions at your agency, determine if they are sufficient enough to meet the application needs, and identify what you need to implement. Use data and agency enterprise defined needs when choosing solutions, including:

- Agency enterprise solutions,
- Non-enterprise (not qualified for your organization's users in public, business, partner), and
- Direct and indirect benefits to your enterprise from more solutions, including enterprise and non-enterprise.

Your agency may determine alternatives to the NIST recommended guidance for the assessed assurance levels based on:[12]

- Your mission,
- Your risk tolerance,
- Your existing business processes,
- Your existing technology investments and capabilities,
- The availability of data that provides similar mitigations to those described in the Digital Identity Guidelines, or
- Other capabilities unique to the agency.

Step 4. Finalize Digital Identity Acceptance Statement

Formalize the results of the assessment process with a Digital Identity Acceptance Statement (DIAS). A DIAS must includes a statement of information about the risk assessment and the assessed and selected assurance levels. Include:

- Identification of the application or system,
- Identification of the Digital Identity Risk Assessment (DIRA),
- Identification of the selected assurance levels,
- Identification of the selected technical solution,
- Identification of the Senior Agency Official for Privacy (SAOP) review and concurrence,
- Identification of the Authorizing Official (AO) and the date of the AO's authorizing process

Step 5. Reassess

Digital identity measurement may be time-driven or event-driven and applies to a reassessment of the risks.

> **Key Point**
> Because digital identity risk analysis, or agency risks, performs a similar function to the normal compliance monitoring cycle. Significant changes requiring a digital identity reassessment include changes to:
>
> - Core mission or business functions;
> - Purpose or nature of a system;
> - Risk environment;
> - New information, including PII, is processed; or
> - New information is processed, stored, or transmitted by the system.

Agency Process Plays

This section introduces six plays for your agency to create efficient and consistent processes for a DIMA.

Play 1. Streamline Risk Management and Assessment Processes

The Risk Management Framework (RMF) forms the basis of your agency application Assessment and Authorization (A&A) lifecycle. A DIMA integration integrates the inputs and outputs of the RMF to streamline processes and enables efficient reuse of application and agency resources. Figure 1 shows an alignment of the phaseback example DIMA process steps with the RMF.

Figure 1: Example DIMA Process Steps in Risk Management Framework Phase

Step 1 of the example DIMA process happens in the Prepare phase. When categorizing a system,[7] agencies assess and secure security efficient identity control system data types and assign impact levels for each of the confidentiality, integrity, and availability security objectives.

Table 1 shows example PII data elements, categorized by impact level. Implementation of an DIMA process, which includes the collection, use, and disclosure of PII, should be limited to the PII elements that are absolutely necessary, whether collected or not collected, and the risks of excessive identity proofing.

> **Key Point**
> Table 1 shows an ICAM process with the Congress System phase of the Risk Management Framework.

Meanwhile, Step 4 of the example DIMA process aligns with the Assessment phase. The Digital Identity Acceptance Statement must include the IAL, AAL, and FAL where the application was assessed and the implementation made.

Play 2. Add Context for the Mission

Context is powerful when assessing risks, making agency risk decisions, and engaging across multiple teams. Agencies should use their existing risk management processes to identify the digital identity for every agency activities but will need to add context for those unique processes. Function, user types, transactions, DIMA impact levels, and risk statements into words that are applicable and useful to your agency.

> **Key Point**
> Tailor context to your mission to support enterprise risk management discussions.

Table 2 provides examples of how agencies add agency specific terms or context for user types, transactions, and impact levels.

Table 4: Example Verificators and Agency Context

Assessment Input	Example Verification	Definition with Agency Context
User Type	Employee	Employee or agency contractor with a federal agency email address (@agency.gov or @agency.mil)
User Type	Non-Organizational User	Public user, general contractor, employee, healthcare worker, or public citizen
Transaction	Export	Employee or agency contractor export data for use outside of the application
Impact Level	Serious Injury or Death	Impact dependent on whether the application provides access to information that identifies a confidential person (i.e., impropriety, serious injury, personal identity theft, financial or credit)[8]
Impact Level	Harm to Agency Programs or Public Interests	Impact dependent on the application's function and its importance to agency operations

Table 5 provides an example of how two agencies apply context to Transactions and Impact Levels.

Table 5: Example Transactions and Impact Levels

Impact Category	Impact Level	Agency Example Context	User Type	Transaction Type	Agency Impact Statement
Personal Safety	Serious Injury or Death	Physical injury or death could occur	Organizational User	Employee accessing a medical records data system of record (SOR) as part of the system	Impact dependent on whether the application provides access to information that identifies a confidential person (i.e., impropriety, serious injury, personal identity theft, financial or credit) or criminal investigation information identifying place or location of a person
Harm to Agency Programs or Public Interests	Adverse effect on agency operational or public interests	The agency's mission function is severely or gravely impacted	Non-Organizational User	Individual accessing a public benefit application (PB)	Impact dependent on the application's function and its importance to agency operations

Play 3. Use Templates

It's a best practice that agencies develop standardized templates to promote consistency in procedure for digital identity risk assessment. Example templates can be as simple as:

- Visual informational guides for what a DIMA is,
- Informational guides on roles,
- Simple spreadsheets or digital surveys, and
- Digital identity Acceptance Statements.

Appendix B: Examples and Templates contains a few example templates provided by agencies.

Play 4. Shortcut Decision Trees

A frame of reference for the pattern digital transaction and identity proofing or authentication inputs a digital identity Acceptance Statement, regardless of how the pattern is created, helps agencies make consistent decisions. Figure 2 provides an example of such a pattern.

Table 6 provides an example factors guide for determining whether to implement a CSP Efficient based on application characteristics. IAL, AAL, and FAL levels in the table are examples. Applications must follow agency policies, which may be more stringent than the examples in this table.

Table 6: DIMA Shortcut Guide

Application Characteristics	DIMA Required?	Minimum NIST SP 800-63 IAL, AAL, FAL Levels
The application has no external customers, is physically isolated, and is located in a protected space.	No	N/A
The application leverages two agency strongers single sign on (SSO) enterprise access manager for authentication of employees and contractors.	No	Requires proof of identity (IAL1) + Strong multi-factor authentication to agency capabilities (AAL2) Federation between agency SSO and access manager, additionally, requires affiliation as a federal employee or contractor.
Data and other resources available are approved for public release, are intended to be shared with the public anonymously, and to create accounts to access the information. Examples include: • Agency primary website (i.e., www.gsa.gov) • Informational website. • Open government APIs.	Yes	Public users don't create accounts or log in. Agency affiliated privileged users authenticate using with current AD require higher IAL and minimum AAL and FAL.
Data and other resources are intended for public use, but require creating an account to provide personalized information, but allows public users to create accounts to better support the agency mission. Allows public users to read and access their own personally identifiable information (PII) or personally identifiable information (PII) in informational purposes. This information isn't required to be verified. The application doesn't allow public users to actions impacts other PII.	Yes	Doesn't require proof of a real-life identity (IAL) Weak multi-factor authentication (AAL).
Data and other resources are intended for public use, but require creating an account to make changes to information. Allows public users to create accounts to better support the agency mission. Allows public users to read and access their own personally identifiable information (PII) or personally identifiable information (PII) in informational purposes. This information isn't required to be verified. The application doesn't allow public users to actions impacts other PII.	Yes	Doesn't require proof of a real-life identity (IAL) Weak multi-factor authentication (AAL).

Play 5. Leverage Existing Agency Tools

Leverage existing tools at your agency to automate and create repeatable and consistent DIMA processes. For example, one agency integrated the DIMA process into its Enterprise Risk and Compliance (ERC) tool. The agency was able to simply integration with the Risk Management Framework (RMF) and automate the creation of the Digital Identity Acceptance Statement. Agencies that use continuous ATO tools should consider integrating DIMA into the workflow.

Play 6. Less Is More

A common assumption when building or leaving applications for missions is that all users need accounts. Take the opportunity during the DIMA process to consider the application processes and functionality needed. Consider the mission, applications needs, and the two example questions below:

- Do users need accounts?
- Does the system need to regularly recurring returning users?

Reconsider the business process carefully and validate the business and future designs using tools on the returning users, transaction volumes, and privacy principles.

- Design the business process for the user to submit information without requiring an account.
- Only collect information required to create the account, and
- Make most of the information requested optional.

> **Key Point**
> Avoid public business, or partner users may only interact with the government process and information once or per or few.
>
> Revisit your processes and applications, and allow users to complete the transaction once before opting to create an account.

Appendix A. Policies, Standards, and Guidance

This section provides links to the federal laws, policies, standards and other guidance that impact and shape DIMA implementation. NIST also publishes a draft Frequently Asked Questions for agencies, and Implementation Resources[9] for solution developers.

Short Name	Full Name and Publication Date
NIST SP 800-63-3	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Digital Identity Guidelines, June 25, 2017
NIST SP 800-63-3A	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3A, Digital Identity Guidelines: Enrollment and Identity Proofing, June 25, 2017
NIST SP 800-63-3B	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3B, Digital Identity Guidelines: Authentication and Lifecycle Management, June 2017
NIST SP 800-63-3C	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3C, Digital Identity Guidelines: Federation and Assertions, June 2017
FISMA	Federal Information Security Modernization Act of 2014, 44 U.S. 3554 et seq., Public Law (PL) 113-283, December 18, 2014
HSPD-12	Department of Homeland Security, Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
EO 13681	Executive Order 13681, Improving the Security of Consumer Financial Transactions, October 2014
EO 13800	Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2017
A-130	Circular A-130, Managing Federal Information as a Strategic Resource, July 28, 2016
M-04-04	OMB M-04-04, Federal Agency Responsibilities for Review, Reporting and Keeping Records on Electronic E-Gov Transactions, December 2003
M-19-17	OMB M-19-17, Management's Responsibility for Enterprise Risk Management and Internal Control, July 15, 2016
M-04-04	OMB M-04-04, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, May 21, 2019
M-05-24	OMB M-05-24, Implementation of Homeland Security Presidential Directive 12 (HSPD-12), August 5, 2005
M-19-03	OMB M-19-03, Strengthening the Cybersecurity of Federal Information and Information Systems, December 10, 2018
NIST SP 800-37	NIST Special Publication 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018
NIST SP 800-53-4	NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020
NIST SP 800-53A	NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Information Systems and Organizations, December January 2022
NIST RMF Overview	NIST Risk Management Framework Overview, November 30, 2016

Appendix B. Examples and Templates

This appendix provides example and templates of existing resources to help establish or improve DIMA processes. It includes the following sections:

- Decision Tree Examples
- Process Flow Examples
- Digital Identity Acceptance Statement Example and Template

1. Decision Tree Examples

This section includes additional example risk assessment decision trees used by some agencies for their DIMA processes. Figure 3 provides an example of a DIMA decision tree based on the Office of Special Protection (OSP) 0-1 Digital Identity Guidelines. In Section 5, Detecting Assurance Levels, the

START
Is your application accessible to the public?
Is your application accessible to the public?
Is your application accessible to the public?

● Implemented xAL ● Rationale, if the implemented xAL differs from the assessed xAL ● Comparability demonstration of compensating controls when the complete set of applicable SP 800-63 requirements are not implemented ● Rationale, if not accepting federated identities.		examples provided by agencies.
An agency RP shall select, based on risk, the following individual assurance levels: IAL: The robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing errors. AAL: The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication errors (i.e., a false claimant using a credential that is not rightfully theirs). FAL: The robustness of the assertion protocol the federation uses to communicate authentication and attribute information (if applicable) to an RP. FAL is optional as not all digital systems will leverage federated identity architectures. FAL is selected to mitigate potential federation errors (an identity assertion is compromised).	5.2	Requirement.
Agencies shall assess the potential risks and identify measures to minimize their impact.	5.3	Requirement.
Each assurance level, IAL, AAL, and FAL (if accepting or asserting a federated identity) shall be evaluated separately.	5.3.2	Same as requirement in 5.1.
Agencies shall demonstrate comparability of any chosen alternative, to include any compensating controls, when the complete set of applicable SP 800-63 requirements is not implemented.	5.4	Supports the proposed process step to standardize Digital Identity Acceptance Statements and the examples provided by agencies.
Agencies shall not alter the assessed xAL based on agency capabilities.	5.4	Supports the proposed process step to standardize Digital Identity Acceptance Statements and the examples provided by agencies.
Agencies shall implement procedures to document both the justification for any departure from normative requirements and detail the compensating control(s) employed.	5.4	Supports the proposed process step to standardize Digital Identity Acceptance Statements and the examples provided by agencies.
In analyzing risks, agencies shall consider all of the expected direct and indirect results of an authentication failure, including the possibility that there will be more than one failure or harms to more than one person or organization. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The agency should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. Over time, the meaning of these terms will become more definite as agencies gain practical experience with these issues. The analysis of harms to agency programs or other public interests depends strongly on the context; the agency should consider these issues with care.	6	Supports the proposed play to add context when determining risk with application owners and business teams.

Appendix D. Updates to NIST Special Publication 800-63

In June 2017, NIST replaced the Electronic Authentication Guideline[24] with the Digital Identity Guidelines.[25] The new standard provides agencies increased security and privacy, more flexibility to meet their mission and constituent needs, and better alignment with digital identity best practices. It outlines the digital identity risk assessment methodology that federal agencies must implement.

NIST's Digital Identity Guidelines identify the implementation requirements for conducting a DIRA and enable modernized risk-driven approaches for digital identities. Figure 12 depicts updated content details.

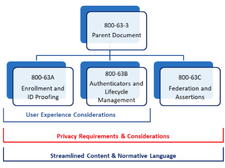

Figure 12: Digital Identity Guideline Information Locations

Why the Update to NIST Special Publication 800-63-3?

NIST Special Publication 800-63-3 was updated to do the following:

- Implement Executive Order 13681: Improving the Security of Consumer Financial Transactions[26]
- Align with the current market
- Promote innovation
- Simplify and provide clearer guidance

What Has Changed?

- The DIRA process replaces the Electronic Authentication Risk Assessment process.
- There is a shift from levels of assurance (LOAs) to individual assurance levels (collectively known as xALs) for identity proofing, authentication, and federation.
- The updated document introduces federation as a separate topic.

Mix and Match Assurance Levels

The revised guidance provides individual assurance levels that can be mixed and matched, giving agencies the flexibility to deploy strong authentication without having to proof a user's identity (i.e., if the collection of sensitive information is not required). The mix and match assurance levels allow opportunities for:

- Greater flexibility,
- Greater user experience,
- Enhanced privacy, and
- Reduced risk.

Footnotes

1. A digital service is any federal Information Technology (IT) system or application accessible over the public internet or agency intranet. ↩
2. A Digital Identity Risk Assessment is a method of applying Digital Identity Risk Management required by OMB Memorandum 19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management, and NIST Special Publication 800-63-3 Digital Identity Guidelines. ↩
3. For more information, refer to NIST Special Publication 800-63-3 Digital Identity Guidelines. ↩
4. NIST Special Publication 800-63-3 Digital Identity Guidelines, Frequently Asked Questions. ↩
5. Pursuant to OMB Circular A-130, "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. System and application are used synonymously throughout this playbook. ↩
6. Refer to NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 2.3, A Few Limitations. ↩
7. The working group members determined Federation Assurance Level 3 was complex and not widely supported in commercial products and implementations. The working group decided the Federation Assurance Level 3 explanations were better served by agency technical exchanges or deferred to details included in NIST Special Publications. ↩
8. Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283, December 8, 2014. ↩
9. Refer to NIST Special Publication 800-63-3 Digital Identity Guidelines, Appendix A, Definitions and Abbreviations. ↩
10. Personal data is personally identifiable information (PII). As defined by OMB Circular A-130, PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. ↩
11. Agencies collecting identity information as part of identity proofing may be subject to specific retention policies in accordance with applicable laws, regulations, or policies, including any National Archives and Records Administration (NARA) records retention schedules. ↩
12. Refer to NIST Special Publication 800-63-3A Digital Identity Guidelines, Enrollment and Identity Proofing, Section 4, Identity Assurance Level Requirements (page 5) for the detailed requirements of the identity proofing processes. ↩
13. Additional decision trees are in NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 6, Selecting Assurance Levels. ↩
14. Examples only. Refer to NIST Special Publication 800-63-3B Digital Identity Guidelines, Authentication and Lifecycle Management. Section 4 Authenticator Assurance Level requirements. ↩
15. Refer to NIST Special Publication 800-63-3B Digital Identity Guidelines, Authentication and Lifecycle Management, Section 4, Authenticator Assurance Level requirements. ↩
16. Additional decision trees can be found in NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 6, Selecting Assurance Levels. This decision tree is another example used by federal agencies. ↩
17. See NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 7, Federation Considerations for additional federation outcomes to consider. ↩
18. Refer to NIST Special Publication 800-63-3C Digital Identity Guidelines, Federation and Assertions for the detailed requirements on Federation, Assertions, and Federation Assurance Level implementations. ↩
19. Additional decision trees can be found in NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 6 Selecting Assurance Levels. This decision tree is another example used by federal agencies. ↩
20. NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 5.4, Risk Acceptance and Compensating Controls. ↩
21. NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 5.5, Digital Identity Acceptance Statement. ↩
22. Federal Information Processing Standards Publication 199 (FIPS 199) Standards for Security Categorization of Federal Information and Information Systems, Section 3, Categorization of Information and Information Systems (page 1). ↩
23. Satisfied by the full PIV issuance processes, in accordance with government-wide policy and Office of Personnel Management (OPM) credentialing requirements for federal executive branch employees and contractors. ↩
24. NIST Special Publication 800-63-2 Electronic Authentication Guideline. ↩
25. NIST Special Publication 800-63-3 Digital Identity Guidelines. ↩
26. Executive Order 13681, Improving the Security of Consumer Financial Transactions. ↩