Digital Identity Risk Assessment Playbook

September 2020

Digital Identity Risk Assessment Working Group

Identity Credential and Access Management Subcommittee (ICAMSC)

Acknowledgements

Table of Contents

Introduction

Digital identity represents each individual engaged in 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 establish that the individual is who they claim to be. Digital authentication provides reasonable risk-based assurances that the individual accessing the application is the same individual who previously accessed the service. This playbook is a method to apply the National Institute of Standards and Technology (NIST) Special Publication 800-63-3 Digital Identity Guidelines. Federal agencies can perform a Digital Identity Risk Assessment (DIRA) to determine the appropriate identity, authenticator, or federation level outlined to access an application.

Purpose

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

DIRAs determine the assurance levels for the digital transactions that involve digital identity or require human authentication.[2] When agencies build or buy applications that use the most current identity proofing and authentication standards, they protect both the digital transactions and the user and agency data behind the applications.

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

- Update and maintain consistent processes;
- Determine whether an agency application requires a DIRA;
- Integrate DIRA into agency Risk Management Framework (RMF) processes; and
- Learn practices to implement DIRA processes.

---

[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.

NIST publishes implementation guides[3] and frequently asked questions (FAQs)[4] for agencies and service providers to use to create information technology *solutions* to meet these standards. This playbook promotes consistency, effectiveness, and efficiency in your agency's processes.

How to Use This Playbook

This playbook is divided into three major sections. Read the entire playbook or jump directly to the section that will help your agency.

- High-Level DIRA Process - Step-by-step guide on how to approach a DIRA process for each agency.
- Agency Process Plays - Six plays to create efficient and consistent processes. For example, Play #4 includes a shortcut decision tree for a streamlined DIRA for some applications.
- Appendices - Example diagrams and templates, and references to policies and standards to use in your agency for communications.

Scope

The DIRA playbook applies to all federal Information Technology (IT) systems and applications that need identity proofing and authentication.[5] This playbook complements the following standard and policy:

- NIST Special Publication (SP) 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

All agency information technology systems should use the DIRA process as part of the Risk Management Framework (RMF) and Federal Information Security Modernization Act (FISMA) processes. Business owners and information security officers produce a Digital Identity Assessment Statement (DIAS) to document the assurance levels determined by collecting and analyzing the system or application data as part of the assessment process.

---

[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 0MB 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.

This playbook does not apply to:

- Non-person entities[6], such as devices, Robotic Process Automation (RPA) or Machine Learning;
- Facilities access;
- Federation Assurance Level 3 solutions[7]; or
- National security systems (NSS)[8].

The following sections describe a basic DIRA process and provide plays to help you implement efficiency into your agency's processes.

High-level DIRA Process

The DIRA process begins when a new application or system is identified or a time-driven or event-driven reassessment is triggered. Once it is determined a DIRA is needed, application data is identified, collected, and analyzed to determine the assurance levels, and produce a Digital Identity Assessment Statement (DIAS), as shown in Figure 1.

---

[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.
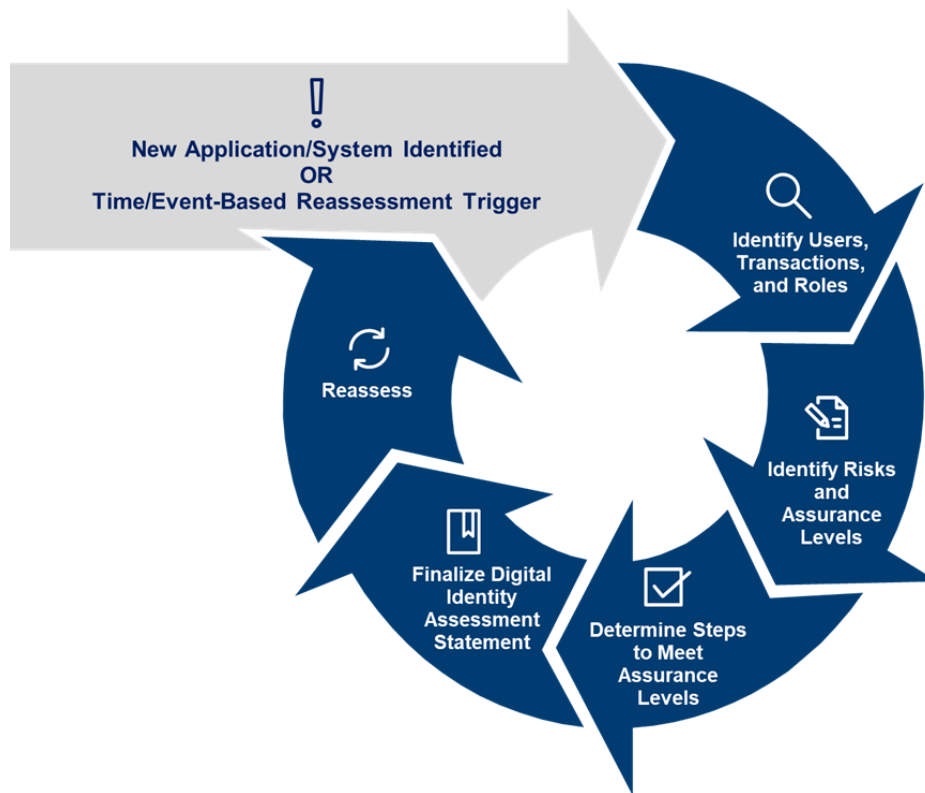
Figure 1: Example DIRA Process

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 Levels
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 business roles of the application.

There are many definitions to categorize users within the federal government, such as:

- User Types - Organizational and Non-Organizational users.
- Communities of Users - Employee, Partner, and Public users.
- Common 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.

Key Point	Identifying categories of users helps define the requirements for more than the Digital Identity Risk Assessments. For example, requirements for privacy, records retention, and monitoring are based on user types and categories.

First, identify the user types and communities of users the application supports. Identifying an application's community of users is important to the DIRA processes as communities have different privacy, regulatory, and solution requirements to consider in risk assessments. Table 1 identifies user types and five common examples of communities of users.

Table 1: Examples of User Types and Communities

User Type	Description	Examples of Community of Users
Organizational	An employee or individual the organization deems to have equivalent status of an employee	Internal agency enterprise 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)	US State, local, and tribal agency users Non-profit, business or commercial users Public or other users

Next, identify each transaction the communities of users can perform in the application.

A transaction[9] is:

> *".. a discrete event between a user and a system that supports a business or programmatic purpose. A government digital system may have multiple categories or types of transactions, which may require separate analysis within the overall digital identity risk assessment."*

---

[9] Refer to NIST Special Publication 800-63-3 Digital Identity Guidelines, Appendix A Definitions and Abbreviations.

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 on data: Create, Read, Modify, Delete.

Key Point	Summarize transactions by each community of users for risk assessments. Each transaction carries a unique set of risks depending on the type of data being accessed and what the user can do with the data.

Finally, map the community of users to the common roles. Most applications have several different user roles, each with different access privileges. Examples of common user roles include:

- **General users**
    - o **Can access:** Information resources provided by the application
    - o **Examples:** Employees, general public
- **Functional privileged users**
    - o **Can access:** Information resources provided by the application, and approval workflows
    - o **Examples:** Managers
- **Information Technology (IT) privileged users**
    - o **Can access:** IT systems with read, write, or change access
    - o **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 Users	Example
Organizational	Other federal government agency users	Agency employee or contractor (User Type) accesses and uploads document to cross-agency collaboration platform (Transaction)
Organizational	Internal agency enterprise user	Agency employee administrator (Role) adds user to an agency's collaboration platform (Transaction)

User Type	Community of Users	Example
Organizational	Internal agency enterprise user	Agency employee or contractor (User Type) exports data for use 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((User Type) searches for national park information and resources (Transaction)
Non-organizational	Public user	Public user (User Type) applies for federal government employment (Transaction)
Non-organizational	Public user	Public user (User Type) 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, common role, and transactions identified in Step 1.

- **Identity Assurance Levels (IALs)** indicate the level of confidence in a claimed identity.
- **Authenticator Assurance Levels (AALs)** indicate authentication requirements.
- **Federation Assurance Levels (FALs)** indicate the level of confidence in an assertion used to communicate identity or authentication information across applications or across agencies.

The risks and impact assessment considers the risks to both the agency and the user for the transactions. The risk to one can be significant, while not negatively impacting the other at all. It's common for government applications to have different assurance levels based on differing impacts and risks for each community of users and transactions.

Key Point	The impact categories and definitions used in the DIRA process are the same used to determine the *overall* application system categorization for impacts 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 authenticator assurance levels for communities of users and transactions for the DIRA.

Table 3 lists the six impact categories to use. This table is a guideline to categorize the risks and impacts involved 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 embarrassment to any party.	At worst, serious short-term or limited long-term inconvenience, distress, or damage to the 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 ordinarily reserved for situations with particularly severe effects or which potentially affect many individuals.
Financial loss or agency liability	At worst, an insignificant or inconsequential financial loss to any party, or at worst, an insignificant or inconsequential agency liability.	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 programs or public interests	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii)	At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

Impact Category	Low	Moderate	High
	minor damage to organizational assets or public interests.		
Unauthorized release of sensitive information	At worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS 199.	At worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS 199.	A release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality 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 risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.	A risk of civil or criminal violations that are of special importance to enforcement programs.

Identity Assurance

Identity Assurance Levels define the processes and solutions used to identity proof users attempting to sign up for a digital service or perform an application transaction. IALs mitigate impacts of 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 you if you aren't?"

Defining the IALs for each community of users and transactions from Step 1 is one of the more challenging aspects of a DIRA. The final IAL correlates to how much personal data[10] is validated and verified for that user during the identity proofing process.[11]

---

[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.

At Identity Assurance Level 1 (IAL1), the application may or may not require proofing. If an application requires input, a user may only need to provide a real or fictitious name for display purposes and an email address to receive notifications. The information may be self-asserted by the user and doesn't need to be verified. At Identity Assurance Level 2 (IAL2) or 3 (IAL3), increasingly more personal information about the user needs to be validated and verified either remotely, supervised remotely, or in-person. At IAL2, a real name, email address, and an address of record are confirmed through record checks remotely or in-person. At IAL3, a biometric is captured and the user 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 explains the three Identity Assurance Levels in *example* terms of the information validated and verified during the identity proofing process.[12]

---

[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.
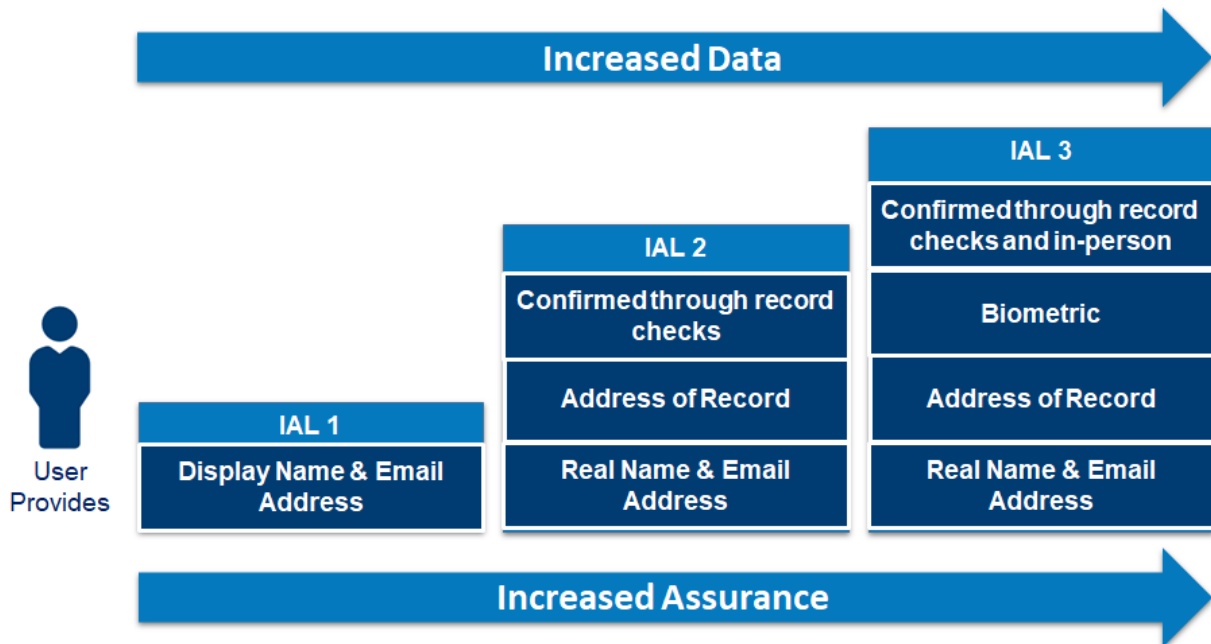
Figure 2: Identity Assurance Levels

Appendix B: Examples and Templates includes an example of a decision tree of the risk assessment process flow that defines the Identity Assurance Levels for the communities of users and transactions in Step 1.[13]

Authenticator Assurance

Authenticator Assurance Levels define the strength of the authentication process. AALs mitigate potential authentication errors (i.e. an attacker accessing a user's account).

- Authenticator Assurance is: "Is this the same user as before?"
- Impacts are: "What are the risks to the government or to you if you aren't?"

At Authenticator Assurance Level 1 (AAL1), a user might only use a username and password. At Authenticator Assurance Level 2 (AAL2), a user has two factors including a factor such as a one-time password (OTP) managed by a mobile application on a personal or government mobile phone[14].

---

[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

	Two-factor authentication is rapidly becoming the expected default for applications.
Key Point	Recurring public and other non-organizational users may want to create an account. Agencies and application owners should strongly consider always allowing and providing two-factor options.
	For employees and other organizational government users, two-factor authentication is a government-wide policy requirement.

Figure 3 explains the concept of the three Authenticator Assurance Levels in *example* terms of the authentication.[15]
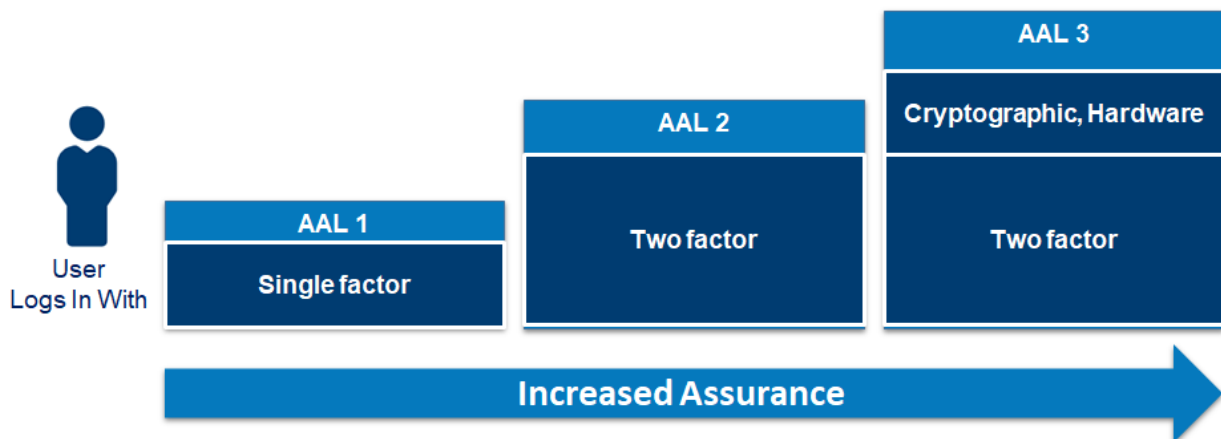
Figure 3: Authenticator Assurance Levels

Appendix B: Examples and Templates includes an example of the risk assessment process flow that defines the Authenticator Assurance Levels for the community of users and transactions in Step 1.[16]

Federation Assurance

Federation Assurance Levels indicate the assertion protocol used by an application to communicate identity and authenticator information. FALs protect information about the *authenticated* user. They mitigate risks if a malicious actor in the transaction changes or replays the information.

---

[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.

Key Point	Federation is an advanced topic with many different acronyms and terms.
	Use outcome-based examples and demonstrations with application owners and business teams to help identify the FALs.

This playbook explains FALs with the outcomes first before explaining the high level requirements and the risk process.[17] To determine if your application requires an FAL, 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 any government or commercial identity provider?
- For organizational government users and transactions, is the application integrated with an employee's network logon?

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

- Do the same users access other agency applications and could the user experience for identity and authentication be streamlined?

If your agency and application owner answers "Yes" to any of these questions, then the application is federated, *or could be federated* during the solution definition step *(Step 3),* and needs a FAL defined for each user community and transaction.

Key Point	Applications that don't implement a federated capability document the rationale in the final Digital Identity Acceptance Statement.
	FAL1 and FAL2 are good for most use cases across the federal government. Agencies and application owners should consider implementations based on the community of users and transactions.

FALs are implemented using standard-based protocols across the federal government. These protocols are commonly used in many applications and transactions globally, and are routinely supported in commercial off-the-shelf (COTS), native cloud software-as-a-

---

[17] See NIST Special Publication 800-63-3 Digital Identity Guidelines, Section 7 Federation Considerations for additional federation outcomes to consider.

service, and consumer and enterprise mobile applications. Each FAL defines <u>minimum</u> requirements for how the integrations are performed, and the requirements if the user's information is passed between applications. For example, for some implementations, the federation assurance levels map to commonly used federation protocols such as OpenID Connect (OIDC) and Security Assertion Markup Language (SAML). How those implementations are done maps to the increasing FAL options.

Figure 4 explains the concept of the three Federation Assurance Levels in *example* terms.[18]
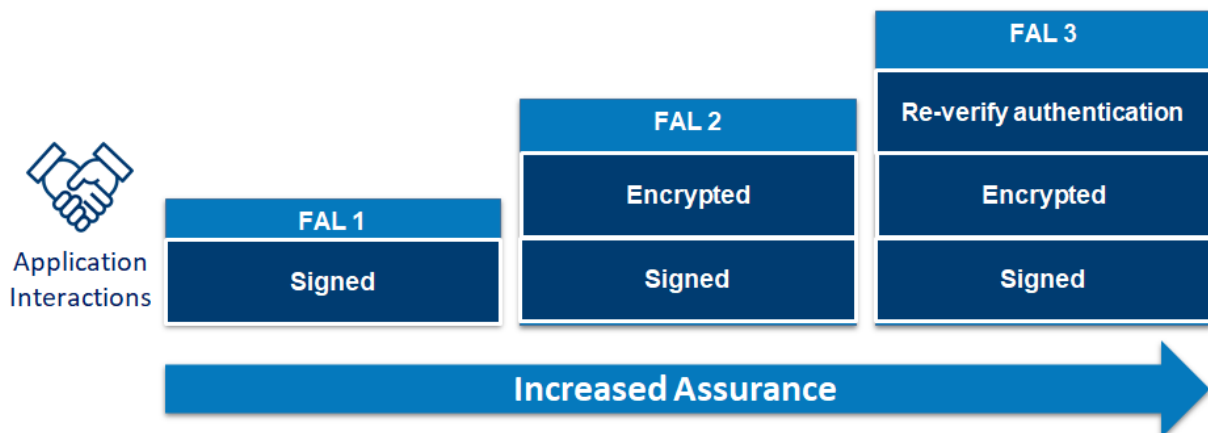
Figure 4: Federation Assurance Levels

Appendix B: Examples and Templates includes an example of a decision tree of the risk assessment process flow that defines the Federation Assurance Levels for the communities of users and transactions in Step 1.[19]

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:

- Number of users by community of users;

---

[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.

- User experience (UX) and usability (for non-organizational users i.e., public, business, partner); and
- Direct and indirect benefits to reuse enterprise-level chosen solutions, including consolidated support desks.

Your agency may determine alternatives to the NIST-recommended guidance for the assessed assurance levels based on your: [20]

- Mission;
- Risk tolerance;
- Existing business processes;
- Special considerations for certain populations;
- 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 include a minimum set of information about the risk assessment and the assessed and implemented assurance levels.[21]

An example of a DIAS is included in Appendix B: Examples and Templates.

Step 5: Reassess

A digital identity reassessment may be time-driven or event-driven and applies to a reassessment of the DIRA.

Key Point	Reassess digital identity risk annually or more often for higher impact categories and transactions. A time-based assessment drives alignment with modernization initiatives, changes to technology, and changes to policies.

---

[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.

If an event triggers a security impact analysis, an agency may perform a DIRA outside the normal continuous monitoring cycle. Significant changes requiring a digital identity reassessment include changes in:

- Core mission or business functions;
- Purpose or nature of a system;
- Risk environment;
- How information, including PII, is processed; or
- How information 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 DIRA.

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 DIRA process integrates into the routine phases of the RMF to streamline processes and enables efficient reuse of application and agency resources. Figure 5 shows an alignment of this playbook's example DIRA process steps with the RMF.
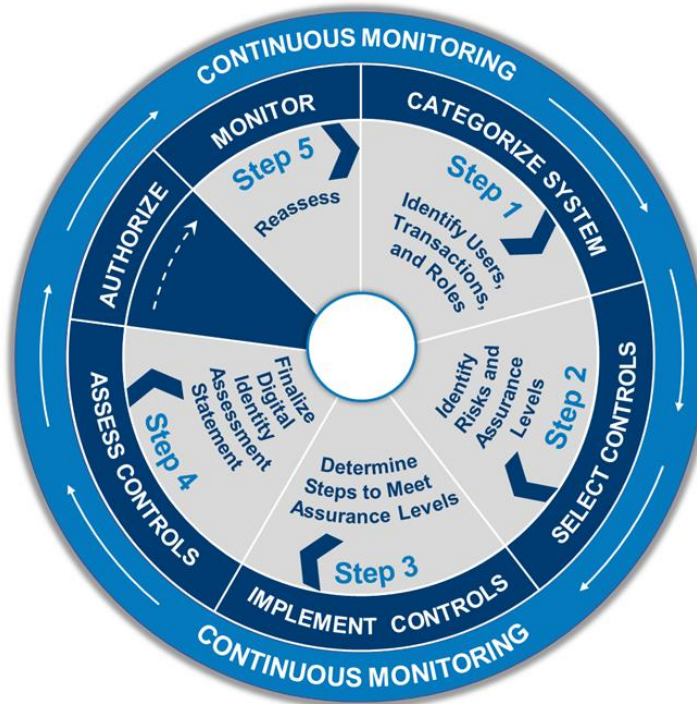
Figure 5: Example DIRA process steps in Risk Management Framework phase

Step 1 of the example DIRA process happens in the Categorize phase. When categorizing a system,[22] application owners and security officers identify overall system data types and assign impact levels for each of the confidentiality, integrity and availability security objectives.

A Privacy Threshold Analysis (PTA) is typically included in this phase. The identification of the DIRA IALs, AALs, and FALs directly correlates to the collection of PII; who has access to what information; whether information is self-asserted or verified; and the risks of excessive identity proofing.

Key Point	
	Align Step 1 in a DIRA process with the Categorize System phase of the Risk Management Framework.

---

[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). .

Meanwhile, Step 4 of the example DIRA process aligns with the Assessment phase. The Digital Identity Acceptance Statement must include the IALs, AALs, and FALs where the application was assessed and the implementations made.

Play #2: Add Context for the Mission

Context is powerful when assessing risks, making agency risk decisions, and engaging across multi-disciplinary agency stakeholders. Standard and general government-wide policies set the foundation for many agency activities, but are written for broad mission areas. Translate user types, transactions, DIRA 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 4 provides examples of how agencies add agency-specific terms or context for user types, transactions, and impact levels.

Table 4: Example Definitions and Agency Context

Assessment Input	Generic Definition	Definition with Agency Context
User Type	Organizational User	Employee or agency contractor with a federal agency email address (@agency.gov or @agency.mil).
User Type	Non-Organizational User	Fiscal agent, Grant beneficiary, Veteran, Healthcare worker, or Public citizen.
Transaction	Export	Employee or agency contractors export data for use outside of the application.
Impact Level	Serious injury or death	Impact depends on whether the application provides access to law enforcement information that identifies a confidential person (i.e., improperly disclosing a confidential person's identity puts them in physical danger).

Assessment Input	Generic Definition	Definition with Agency Context
Impact Level	Harm to Agency Programs or Public Interests	Impact depends 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	Scope of Potential Risk	Agency Context: As a result of a wrong user accessing data in an application, …	User Type	Transaction Type	Agency Impact Definition
Personal Safety	Serious injury or death	Physical injury or death could occur	Organizational User	Employee or agency-contractor exports data for use outside of the system	Impact depends on whether the application provides access to law enforcement information that identifies a confidential informant (i.e., improperly disclosing a confidential criminal informant's identity puts them in physical danger)
Harm to Agency Programs or Public Interests	Adverse effect on organizational operations	The agency's mission essential functions is adversely impacted	Non-Organizational User	Individual retrieves tax information (PII)	Impact depends 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 procedures for digital identity risk assessments. Example templates can be as simple as:

- Visual informational guides for what a DIRA is;
- Informational guides on risks;
- 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

All federal applications that perform digital transactions and require identity proofing or authentication require a Digital Identity Acceptance Statement, regardless of how the system is hosted. However, not all federal applications require the full example DIRA process and efforts.

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

Table 6: DIRA Shortcut Guide

Application Characteristics	DIRA Required	Minimum NIST SP 800-63 IAL, AAL, FAL Levels
The application has no external network connectivity, is physically isolated, and located in a protected space.	No	N/A
The application leverages the agency enterprise single sign on (SSO) / enterprise access manager for authentication of employees and contractors.	Yes	Requires proof of identity (IAL3[23]). Multi-factor authentication to agency application (AAL2) Federation between agency applications (FAL2) Additionally, requires affiliation as a federal employee or contractor.
Data and other resources available are	No	Public users don't create

---

[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.

Application Characteristics	DIRA Required	Minimum NIST SP 800-63 IAL, AAL, FAL Levels
approved for public release, are intended to be freely shared, and public users aren't required to create accounts to access this information. Examples include: • Agency primary websites (i.e., www.gsa.gov), • Informational websites, and • Open government APIs.		accounts or login. *Agency-affiliated privileged users with permissions to edit content still require higher IAL and a minimum AAL2 (two-factor).
Data and other resources are intended for public release. Doesn't include any controlled unclassified information, but allows public users to create accounts to better support the public user's experience.	Yes	Doesn't require proof of a real-life identity (IA 1). Single or multi-factor authentication (AAL1).
Allows public users to input and access their own personally identifiable information (PII) or protected health information (PHI) for informational purposes. The information isn't required to be verified. The application doesn't allow public users to access anyone else's PII or PHI.	Yes	Doesn't require proof of a real-life identity (IAL1). Multi-factor authentication (AAL2).

Play #5: Leverage Existing Agency Tools

Leverage existing tools at your agency to automate and create repeatable and consistent DIRA processes.

For example, one agency integrated the DIRA process into their Governance Risk and Compliance (GRC) tool. The agency was able to simplify integration with the Risk Management Framework (RMF) lifecycle and support the inclusion of the DIAS with other system artifacts. Agencies that use commercial GRC tools should consider integrating DIRAs into the workflows.

Play #6: Less is More

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

1. Do all users need accounts?
2. How many users are regularly *recurring returning* users?

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

- Design the business process for the user to submit information <u>without requiring</u> an account;
- Limit the information required to create the account; and
- Make most information requested optional.

Key Point	Some public, business, or partner users may only interact with the government process and application once a year <u>or less</u>.
	Revisit your process and application, and allow users to complete the transaction once before opting in to create an account.

Appendix A: Policy, Standards, and Guidance

This section provides links to the federal laws, policies, standards and other guidance that impact and shape DIRA implementations. NIST also publishes useful Frequently Asked Questions for agencies, and an Implementation Resource for solution developers.

[NIST SP 800-63-3]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3; Digital Identity Guidelines, June 22, 2017
[NIST SP 800-63-3A]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3; Digital Identity Guidelines: Enrollment and Identity Proofing, June 22, 2017
[NIST SP 800-63-3B]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3; Digital Identity Guidelines: Authentication and Lifecycle
[NIST SP 800-63-3C]	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3; Digital Identity Guidelines: Federation and Assertions, June 22, 2017
[FISMA]	Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283, December 8, 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]   OMB Circular A-130, Managing Federal Information as a
                    Strategic Resource, July 28, 2016.

[A-108]   OMB Circular A-108, Federal Agency Responsibilities for Review,
                    Reporting, and Publication under the Privacy Act, December
                    2016

[A-123]   OMB Circular A-123, Management's Responsibility for Enterprise
                    Risk Management and Internal Control, July 15, 2016.

[M-19-17]   OMB M-19-17, Enabling Mission Delivery through Improved
                    Identity, Credential, and Access Management, May 21, 2019.

[FIPS 199]   Standards for Security Categorization of Federal Information
                    and Information Systems, February 2004.

[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 4, Security and
                    Privacy Controls for Federal Information Systems and
                    Organizations, April 2013 (Updated 1/22/2015).

[NIST SP 800-53A]   NIST Special Publication 800-53A, Assessing Security and
                    Privacy Controls in Federal Information Systems and
                    Organizations: Building Effective Security Assessment Plans,

July 2008.

[NIST RMF Overview]   Risk Management Framework Overview, November 30, 2016.

Appendix B: Examples and Templates

This section provides examples and templates of existing resources to help establish or improve DIRA processes.

In this section, you'll find links to:

1. Decision Tree Examples
2. Process Flow Examples
3. 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 the Digital Identity Risk Assessment for transactions. Original source decision trees are in NIST Special Publication 800-63-3 Digital Identity Guidelines, *Section 6 Selecting Assurance Levels*.
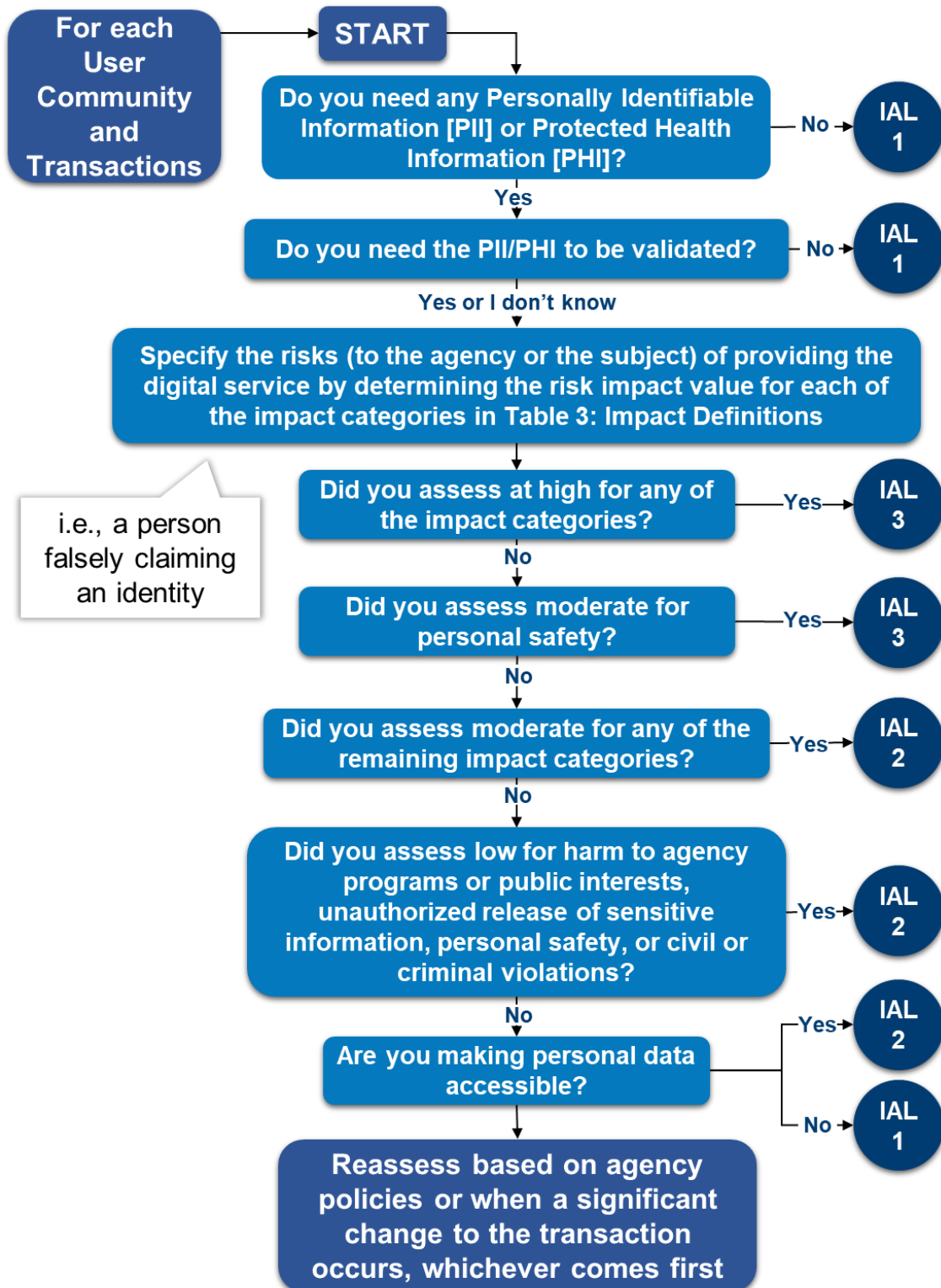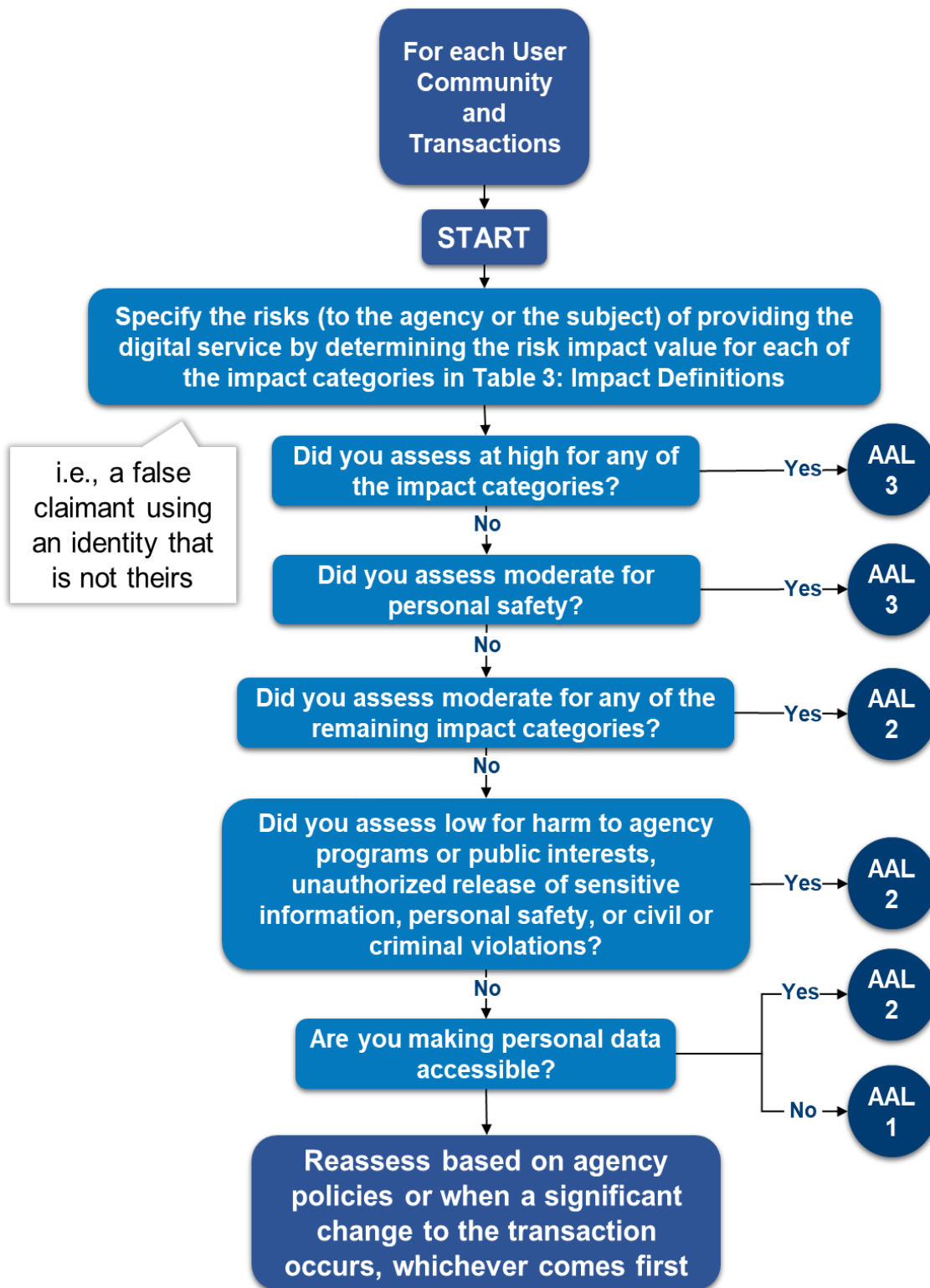
Figure 6: Identity Assurance Level Decision Tree

Figure 7: Authenticator Assurance Level Decision Tree

For each User Community and Transactions

START

Are you federating? — No → **No FAL assessment required**

Specify the risks (to the agency or the subject) of providing the digital service by determining the risk impact value for each of the impact categories in Table 3: Impact Definitions

i.e., an identity assertion is compromised

Did you assess at high for any of the impact categories? — Yes → **FAL 3**

No

Did you assess moderate for personal safety? — Yes → **FAL 3**

No

Did you assess moderate for any of the remaining impact categories? — Yes → **FAL 2**

No

Did you assess low for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations? — Yes → **FAL 2**

No

Are you making personal data accessible? — Yes → **FAL 2**

No

Are you using a front channel? — Yes → **FAL 2**

No → **FAL 1**

Reassess based on agency policies or when a significant change to the transaction occurs, whichever comes first
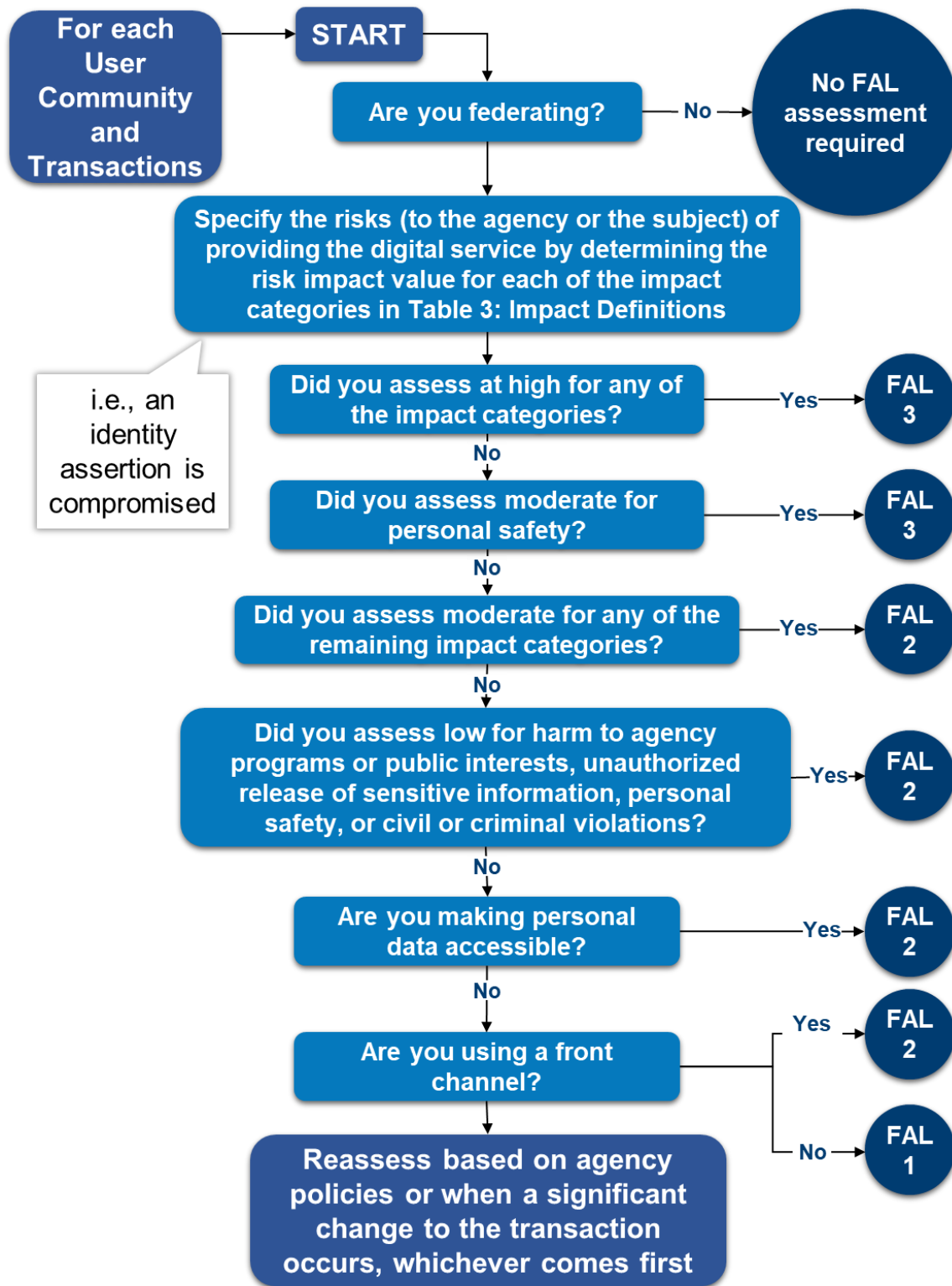
Figure 8: Federation Assurance Level Decision Tree

2. Process Flow Examples

This section includes additional example process flow diagrams used by some agencies for the Digital Identity Risk Assessment processes. Choose and reuse any process flow that works best for your agency.
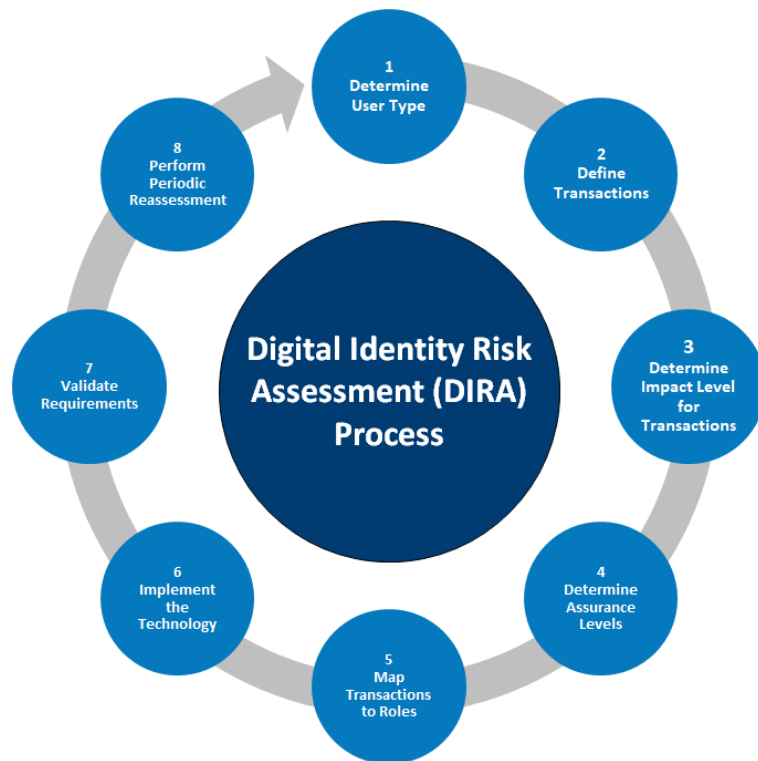

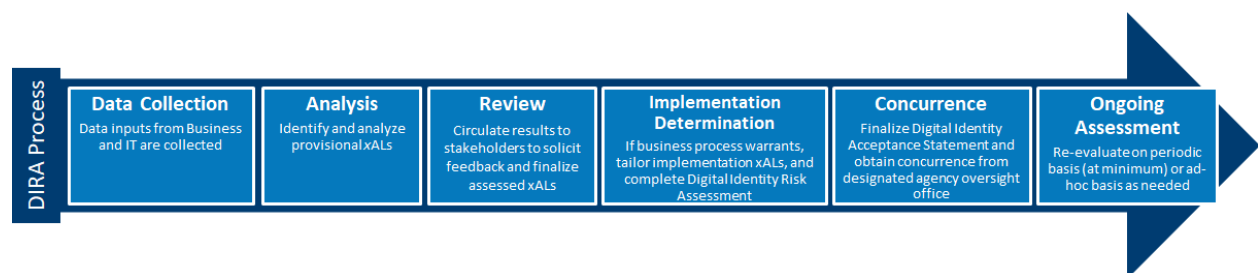**Figure 9. Explains the DIRA process from Data Collection to the Outgoing Assessment**.

Figure 10. Explains in a more detailed way the DIRA Process Flow from Data Collection phase to the Outgoing Assessment phase.
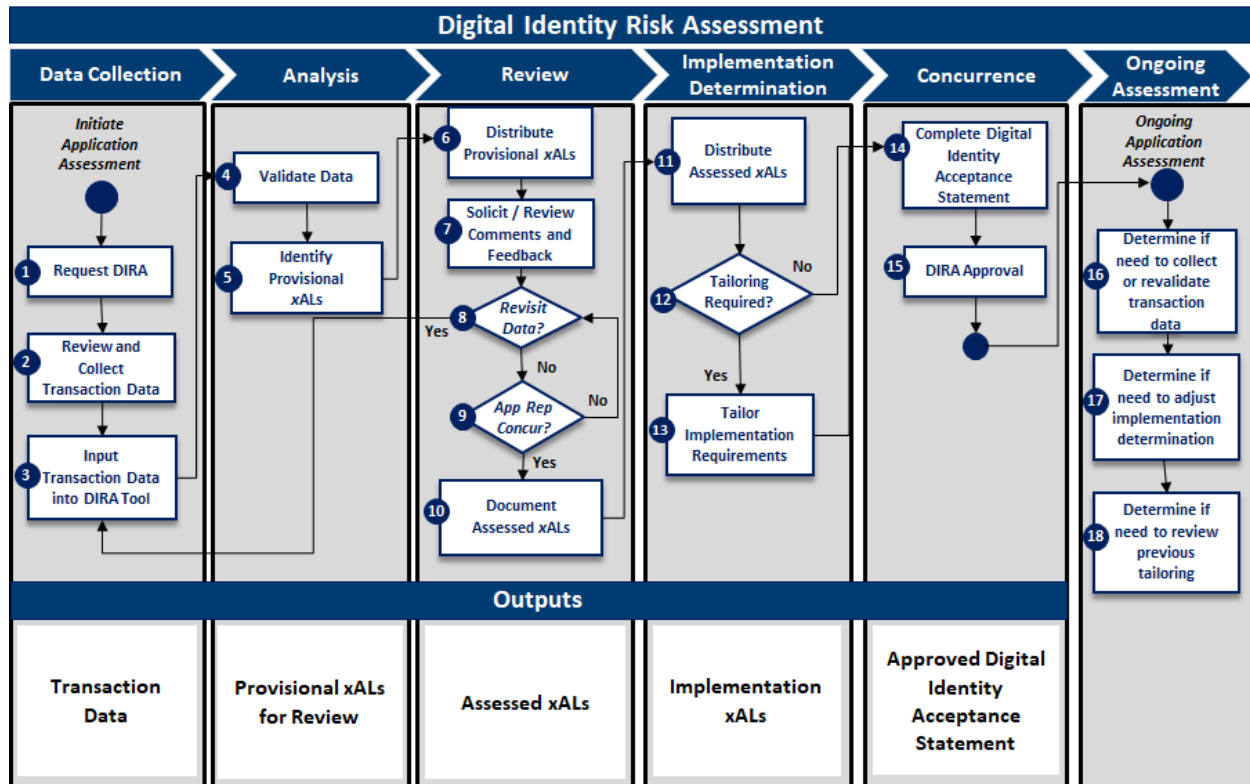
Figure 11: Explains a six step process of what is required to implement a DIRA.

3. Digital Identity Acceptance Statement Example Template

This Digital Identity Acceptance Statement template is provided as one sample for agencies.

Digital Identity Acceptance Statement

In accordance with the provisions of the Federal Information Security Modernization Act, the National Institute of Standards and Technology (NIST) Special Publication 800-63-3 *Digital Identity Guidelines,* and [Agency Policy], a risk assessment was performed for the [SYSTEMNAME] [FISMA ID].

Date	
Agency	
System Name	
FISMA ID	

Program Manager / System Owner	
Information System Security Manager	
Authorizing Official	
Chief Information Security Officer	
Chief Privacy Officer / Senior Agency Official for Privacy	

This acceptance statement identifies the users, transactions, and the assessed and implemented assurance levels for:

- Identity Assurance (IAL)
- Authenticator Assurance (AAL)
- Federation Assurance (FAL)

User Type and Transaction	Description	Assurance Level	Assessed	Implemented
		IAL		
		AAL		
		FAL		
		IAL		
		AAL		
		FAL		

[*If an implemented value is less than the assessed value, identify the compensating controls or agency rationale. Delete if not applicable.*] Compensating controls were implemented for the following user types and transactions:

User Type and Transaction	Assurance Level	Description of Compensating Controls or Agency Rationale

[*If a federation assurance level is marked as Not Applicable, identify the agency rationale.*] Federated identity was not used for all user types and transactions:

Rationale if not implementing federated identities

Appendix C: NIST SP 800-63-3, Requirements Traceability Matrix

This appendix includes <u>both</u> normative requirements and informative references from NIST SP 800-63-3: *Digital Identity Guidelines*. Only requirements related to the agency processes for digital identity risk assessments are included. The playbook consideration column includes comments on the standards statements and alignment to this playbook's development.

Requirement	Section	Playbook Consideration
Applicability: Not all digital services require authentication or identity proofing. However, this guidance applies to all such transactions for which digital identity or authentication are required, regardless of the constituency (i.e., citizens, business partners, government entities).	2.1	Supports the proposed process recommendations to independently assess the assurance levels by the community of users.
Additionally, federal agencies implementing these guidelines should adhere to their statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283 [FISMA], and related NIST standards and guidelines. FISMA directs federal agencies to develop, document, and implement agency-wide programs to provide security for the information and systems that support the agency's operations and assets. This includes the security authorization and accreditation (SA&A) of IT systems that support digital authentication.	2.1	Supports the proposed DIRA process step recommendations to align with the Risk Management Framework and SA&A of IT systems.
Requirements contained herein provide specific guidance related to digital identity risk that agency RPs SHALL apply while executing all relevant RMF lifecycle phases	5	Supports the proposed DIRA process step recommendations to align with the Risk Management Framework and SA&A of IT systems.
Agencies shall assess the risk of proofing,	5.1	Supports the proposed process

| Requirement	Section	Playbook Consideration
authentication, and federation errors separately to determine the required assurance level for each transaction		recommendations to independently assess the assurance levels by the community of users and transactions.
Agencies shall develop a "Digital Identity Acceptance Statement", in accordance with SP 800-53A IA-1 a.1. See Section 5.5 for more detail on the necessary content of the Digital Identity Acceptance Statement. The Acceptance Statement shall include at a minimum: • Assessed xAL. • 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.	5.1 5.5	Supports the proposed process step to standardize Digital Identity Acceptance Statements and the 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	5.2	Requirement.

Requirement	Section	Playbook Consideration
will leverage federated identity architectures. FAL is selected to mitigate potential federation errors (an identity assertion is compromised).		
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	6	Supports the proposed play to add context when determining risk with application owners and business teams.

Requirement	Section	Playbook Consideration
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.		

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.

---
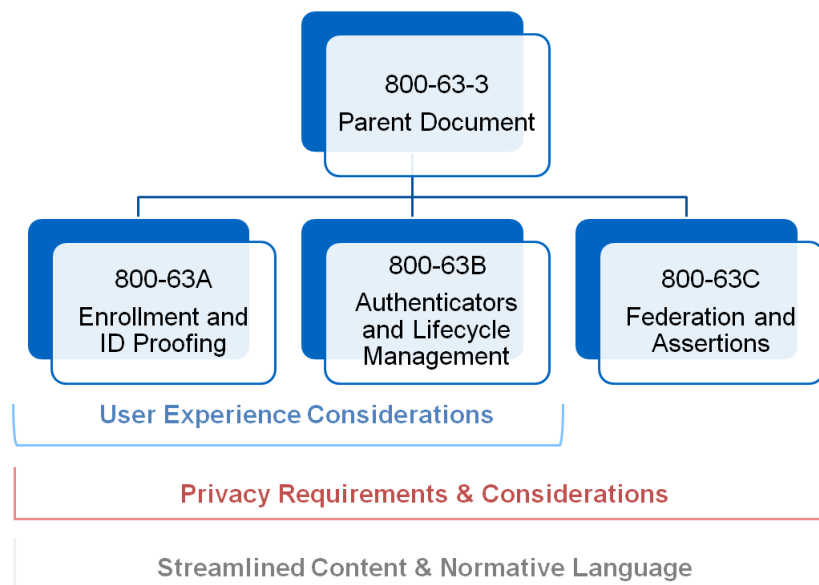
[24] NIST Special Publication 800-63-2 Electronic Authentication Guideline.
[25] NIST Special Publication 800-63-3 Digital Identity Guidelines.

Figure 12: Explains where the Digital Identity Guidelines information can be found.

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

- 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.
- Shift from levels of assurance (LOAs) to individual assurance levels (collectively known as xALs) for identity proofing, authentication, and federation.
- 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.

Pre-Draft Call for Comments on NIST Special Publication 800-63-3

In June 2020, NIST released a pre-draft call for comments to update NIST Special Publication 800-63-3.

---

[26] Executive Order 13681, Improving the Security of Consumer Financial Transactions.