WHITE PAPER

DECIPHERING DIGITAL IDENTITY GUIDELINES IN NIST SP 800-63 R4 FOR FINANCIAL INDUSTRY

Abstract

The financial services sector is a crucial component of the nation's infrastructure. Financial institutions are always considered high-risk and are under constant regulatory pressure as they are prime targets for any cyber-attacks. Considering the sensitivity of the industry, any financial institution should have governance and risk compliance process at its core, ensuring operational resilience to prevent any cyber-attacks including having a diligent incident response in place. With growth of online services, the need for secure, private, and equitable digital identity solutions is intensified.

Regulatory frameworks help achieve risk reduction, regulatory alignment, operational efficiency and stakeholder confidence. **NIST-CSF** is one such framework that helps unify, map disparate regulatory requirements into a coherent cybersecurity strategy. This framework is flexible and scalable, allowing institutions of all sizes to tailor it to their risk profile, infrastructure, and maturity level. Several financial institutions follow NIST-CSF framework globally. It is important for financial institutions to stay up to date with framework changes to ensure risk prevention and enhance resilience against potential cyberattacks. Recently, NIST released the final version of updated Digital Identity Guidelines (SP 800-63). This paper delves into key implications of NIST SP 800-63 R4 for financial institutions, and best practices that need to be followed to minimize the threat for the organization based on NIST framework.

NIST SP 800-63-4 focuses on identity proofing, authentication, and federation. It introduces a risk-based framework and strengthens requirements for privacy, accessibility, and phishing-resistant authentication.

Infosys®
Navigate your next

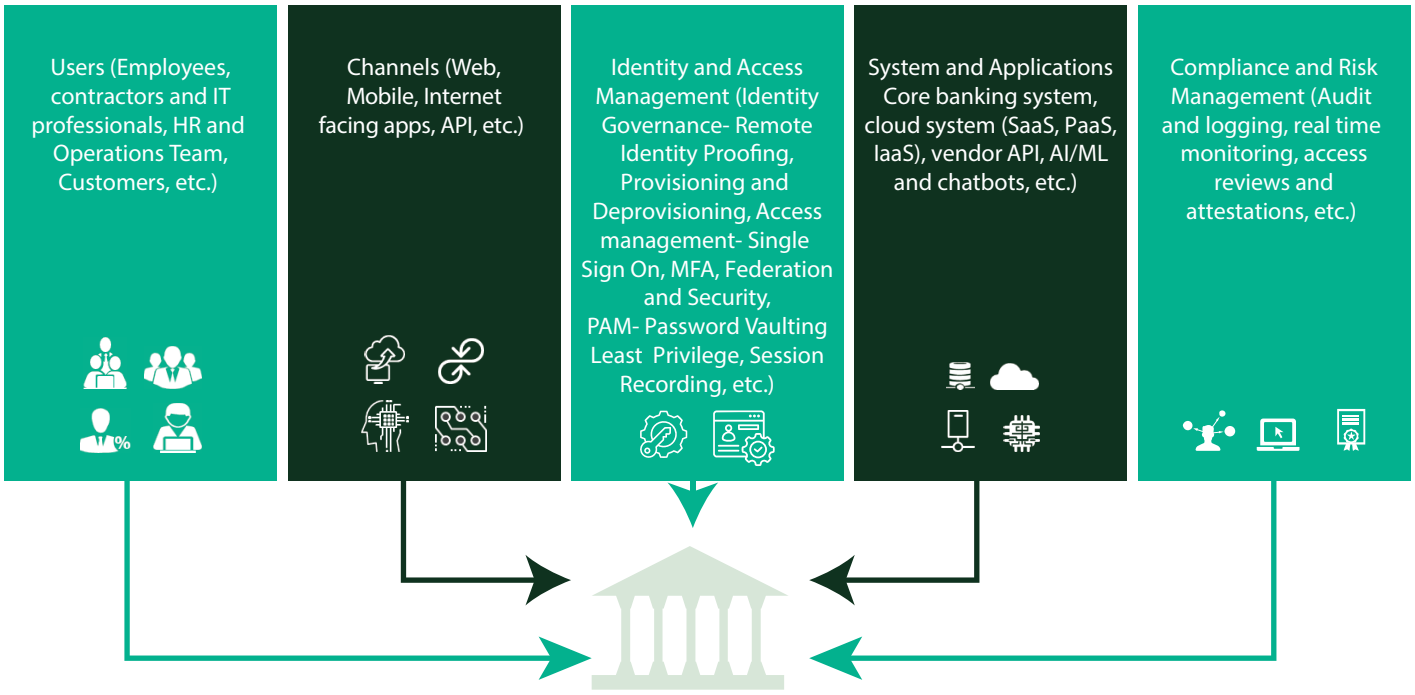
Cybersecurity – Strategic Imperative for Financial Sector

In August 2025, NIST released the final version of SP 800-63, Revision 4 (SP 800-63-4) of its Digital Identity Guidelines for public review, aiming to address the realities of rapidly evolving digital threats, privacy requirements, and equity concerns in digital identity management.

In this whitepaper, we will broadly deal with the evolving threats and their remediation.

Key Actors and Systems Involved

The diagram below illustrates the various actors and systems that interact with each other on a day-to-day basis within a financial organization.



Key Challenges in implementing guidelines of NIST 800-63 R4 for Financial Institutions

The presence of outdated or legacy core banking systems finds it hard to retrofit security into IAM capability enablement as per NIST guidelines. Features such as continuous monitoring and vigilance for threat detection across the systems are lacking in most of the financial organizations. Due to the rapid adoption of cloud-native banking, AI/ML, blockchain, and open banking APIs, it becomes difficult to map the security controls to the shared responsibility models of cloud providers.

In addition, absence of proper risk management systems and lack of secured remote identity proofing mechanism results in identity theft and fraud within the financial ecosystem.

Following figure depicts the identity-related risks associated with financial sectors as per NIST 800-63 R4:

Credential Compromise

Attackers trick users into revealing the credentials using phishing and social engineering. Despite stronger recommendations, weak passwords remain exploitable. Sometimes, due to compromised authenticators (such as stolen hardware tokens or SMS code interceptions), there is an identity risk.

Recommendation as per NIST:
As per guidelines of NIST SP-800-3B, it requires stronger authenticators and phishing resistant MFA (like FIDO2 and PKI).

Identity Proofing & Fraud

Fraudsters combine stolen and fake data to pass the Identity proofing along with document forgeries using AI- driven technologies.

Recommendation as per NIST:
Stronger evidence validation, biometric verification and anti-spoofing is required as per NIST SP-800-63A to remediate the risk.

Privacy & Data Breaches

Identity data leakage is a common scenario where the PII information of individuals are exposed from IdPs, CSPs or relying parties. Sometimes due to irrelevant passing of excessive attributes can lead to serious privacy breach.

Recommendation as per NIST:
As per NIST SP-800-63 (Privacy), Data minimization by limiting the passing of only relevant attributes as claims need to be passed along with consent from user for sharing their information with the required provider.

Federation & Assertion

Stolen SAML/OIDC assertion tokens are reused by attackers which is a very common phenomenon to manipulate tokens or JWT claims to escalate privileges.

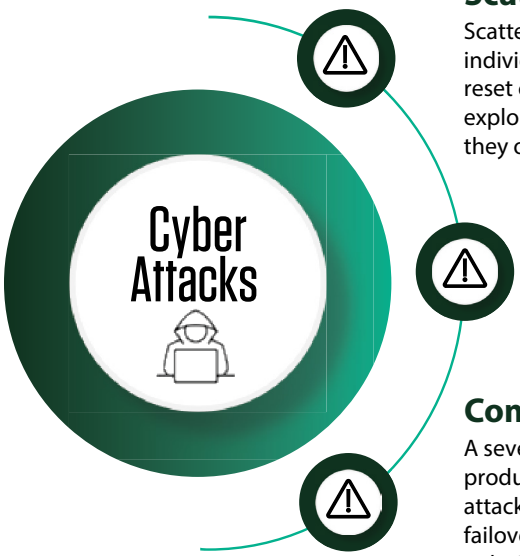
Recommendation as per NIST:
Requires assertion binding, audience restriction and secure key management using stronger Assertion Security methodologies.

Session Hijacking/Recovery

Exploiters steal session cookies, tokens and TLS sessions for active users along with replay attacks. Attackers exploit password reset and account recovery workflows causing account recovery exploitation. The Orphaned accounts also create unauthorized access posing risks.

Recommendation as per NIST:
As per guidelines from NIST SP-800-63B and C, session binding to devices and TLS enforcement with stronger recovery workflow must be as strong as initial enrollment.

Recent IAM cyber-attacks and its Impact



Scattered Spider (LUCR3) attack

Scattered spider hits directly at IAM systems and controls specially targeting the high-level individuals (especially C-suite) and use detailed reconnaissance to convince helpdesk staff to reset credentials. Once they are able to get inside the IAM system using MFA codes, they exploit privileged platforms to escalate access, persist and move laterally. After Identity breach, they often pivot to critical infrastructure to deploy ransomware or mass-impact systems.

Supply Chain/OAuth Token Attack

Scattered spider hits directly at IAM systems and controls specially targeting the high-level individuals (especially C-suite) and use detailed reconnaissance to convince helpdesk staff to reset credentials. Once they are able to get inside the IAM system using MFA codes, they exploit privileged platforms to escalate access, persist and move laterally. After Identity breach, they often pivot to critical infrastructure to deploy ransomware or mass-impact systems.

Compromised Credentials - Scattered Lapsus$ Hunters

A severe cyberattack recently forced an auto-manufacturer to shut down major IT and production systems creating large supply chain and economic impacts. Reports indicate attackers targeted systems that intersect IT and factory/OT operations, making recovery and failover complex. Adversaries that gain administrative access in IT can reach OT control points or build the conditions that cause production outages. IAM compromise is a credible path to operational disruption.

Why adopt it, and why it matters?

A financial institution must follow the NIST-CSF regulatory framework. If not, they can expose the organization to several significant risks. A few such risks of not using the NIST Framework at all are:

Increased vulnerability to cyber threats	Regulatory non-Compliance	Reputational damage	Inefficient risk management	Operational disruption

If a financial institution is using an outdated version of the NIST-CSF SP 800-63 Framework, they are most likely to face the following risks:

Misalignment with the current threat landscape, increasing the risk of cyberattacks	Major gaps in governance and risk management	Non-compliance with regulatory requirements	Limited scope and flexibility	Missed opportunities for improving resilience

Why NIST-CSF framework adoption matters to a financial organization can be understood better by using the below example:

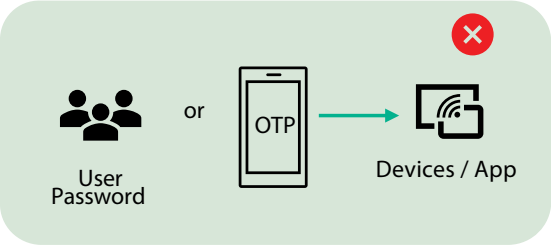
Scenario: An organization is using an outdated NIST-CSF framework and specifically sticking with AAL1 instead of upgrading to AAL2, in the context of session timeout and authentication.

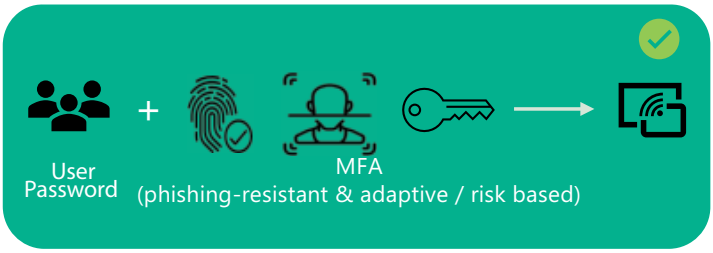
Current use of AAL1:

In this example, a financial institution currently uses Authenticator Assurance Level 1 (AAL1) for user authentication. This level permits single-factor authentication, such as passwords or OTPs, and has longer session timeout periods due to less stringent reauthentication requirements. This could lead to weak authentication, session hijacking, non-compliance, possible data exposure. This eventually creates risk, making the institution more prone to cyber-attacks, reputational damage, and leads to compliance issues.

How AAL2 improves security:

Having AAL2, as mandated in NIST SP 800-63-4, ensures stronger authentication for systems handling sensitive data by requiring multi-factor authentication (MFA). It mandates two distinct authentication factors (e.g., password + hardware token or biometric), secure session management (shorter session timeouts), cryptographic requirements, phishing-resistant authenticators.





What's changing in NIST SP 800-63 Release 4?

NIST SP 800-63 R4 reflects today's rapidly evolving digital threat landscape, privacy requirements, and equity goals. It modernizes identity proofing, authentication, and federation processes to meet current and future needs. This revision comes at a crucial time, as the rapid growth of online services has intensified the need for secure, private, and equitable digital identity solutions.

NIST has provided guidelines in four iterations focusing on critical areas of digital identity as below:

- Digital Identity Guidelines (SP 800-63-4)
- Identity Proofing & Enrollment (SP 800-63A)
- Authentication & Authenticator Management (SP 800-63B)
- Federation & Assertions (SP 800-63C)

The table below summarizes key updates from NIST SP 800-63-3 (2017) to NIST SP 800-63-4 (2024/2025):

Area	SP 800-63-3 (2017)	SP 800-63-4 (2024/2025)
Accessibility	Limited	Explicit equity and inclusion standards
Identity Evidence	ID docs, biometrics (limited)	Adds new technologies, verifiable credentials, better biometrics
Assurance Levels	IAL, AAL, FAL (Levels 1-3) was introduced, where Level1 provided with minimal protection, Level 2 with medium strength and Level 3 with strongest strength	IAL, AAL and FAL (Levels 1-3) have been more refined with more nuanced proofing categories, fraud controls, tightened phishing-resistant and stronger assertion protections.
Authentication	MFA suggestions, SMS OTP allowed	Phishing-resistant MFA required at AAL2+, passkeys
Passwords	Complexity, resets suggested	Length & compromise check, removes complexity/reset
Federation	Loose assertion requirements	Federated logins must use direct cryptographic auth
Risk-based auth	Informal, rare	Explicitly supported/advised for transactions
Recovery	Basic, non-standardized	Improved and formalized recovery procedures

Our view on NIST SP 800-63-4 Adoption

The changes are broadly categorized into four critical areas of digital identity, and each area has mandatory and optional changes. Adopting each of these changes immediately could be challenging for any organization. Considering this, the view is based on the assumption that the organization is already following the NIST-CSF framework (including SP 800-63-3) and is expected to implement or adopt the 2025 changes. We have categorized our view into three areas:

Immediate analysis and implementation target areas where assessments can be performed easily and changes can be applied quickly. It must include analysis of the current assurance levels that will help improve the security of the organization.

Assessment & implementation in the medium term is focused mainly on the areas of digital identity guidelines, fraud detection, federation, and assertion, particularly those that would require more time as some considerations could be new for the organization and implementation is expected to take more time.

Long-term goals are focused mainly on identity proofing and enrollment, as this requires a detailed analysis of the current identity validation process. The latest changes are to be incorporated considering adoption, privacy, and usability-related aspects, and implementation is expected to need more time.

It should be tailored based on organization's current state of IAM solution, business priorities and risk profile. As an example, guidelines marked in Medium or Long Term (such as Identity Proofing) can be moved to capability block for Immediate implementation.

Analyze & Implement
- Immediate

1. Risk Management Framework (Including analysis of assurance levels)
2. Password Guidelines
3. Multi-Factor Authentication (MFA)
4. Authenticator Lifecycle Management
5. Federation Protocols
6. Phishing-Resistant Authentication

Asses & Implement
- Medium Term

1. Equity & Inclusion
2. Privacy Enhancements
3. Usability Considerations
4. Assertion Security
5. Privacy in Federation
6. Interoperability

Strategic
- Long Term

1. Migration Of Identities
2. Remote Identity Proofing
3. Biometric Collection
4. Identity Evidence Validation
5. Fraud Detection

NIST SP 800-63-4 - Focus Areas

Digital Identity Guidelines (SP 800-63-4)

The overarching guidelines in SP 800-63-4 introduce various important changes:

Areas / Guideline / Framework	What's Changing?	How could this be addressed?
Risk Management Framework	A new approach to assessing and managing digital identity risks, emphasizing flexibility and adaptability to various organizational contexts. Moves beyond static compliance to continuous, context-aware identity risk management.	• Align Risk Management Framework with Digital Risk Management Framework principles enabling dynamic control selection, based on context, threats, and assurance levels (IAL, AAL, FAL). • Ensure real-time identity risk evaluation, supporting Zero Trust and continuous verification. • Ensure risk management frameworks consider privacy and equity considerations, leverage AI/ML tools to automate risk assessments, and map assurance levels directly to control baselines. • Ensure support for verifiable credentials and digital wallets.
Equity and Inclusion	Enhanced focus on ensuring digital identity solutions is accessible and fair to all users, regardless of their demographics or technological access.	• Enforce inclusive design practices that support accessibility and assistive technologies, with a focus on digital identity.
Privacy Enhancements	Strengthened measures to protect user privacy, including minimizing data collection and improving transparency in identity processes.	• Analyze the user information currently being collected and ensure that only the absolute minimum is collected and utilized. Improve transparency regarding user data collection and its usage. • Check the information shared during assertion to reduce it to absolute minimum. • Using AI-based Analytics will help in eliminating the user's data compromise from the intruders by limiting access to individuals on a near real time basis.
Usability Considerations	Greater emphasis on designing digital identity systems that are easy to use, without compromising security.	• Current policies on user consent, privacy, and control must be reassessed. • Authentication systems must be assessed and should adopt interoperable methods, meet accessibility standards, and support syncable authenticators such as passkeys. • Existing MFA setups need to be tested and upgraded to phishing-resistant MFA
Migration of Identities	Covers scenarios like updating credentials, transitioning to new authentication methods (a form of migration), and managing identity assurance levels over time.	• Analyze Identity Assurance level to ensure compliance, redefine and implement, as appropriate. This includes strengthening digital identity risk management processes.

Identity Proofing & Enrollment (SP 800-63A)

SP 800-63A outlines following substantial updates to identity proofing and enrollment processes:

Areas / Guideline / Framework	What's Changing?	How could this be addressed?
Remote Identity Proofing	Expanded guidelines for remote identity verification reflect the increased demand for online services.	• Analyze and compare the existing policies for identity verification and analyze / plan on how this can be expanded for Remote Users Onboarding and verification. • Emphasize cross-checking and implementation of fraud detection mechanisms. • Encourage / mandate real-time liveness detection and anti-deepfake technologies. • Use of AI/ML needs to be encouraged to strengthen identity verification at the helpdesk to counter Scattered Spider-style social engineering attacks. AI/ML usage could help reduce intervention and errors and as a result it will help improve response speed while maintaining high assurance levels.
Biometric Collection	Revised standards for biometric data collection and usage aim to balance security requirements with privacy concerns.	• Analyze the existing policy for privacy, biometric data collection, storage, usage and how it is integrated with HR, banking systems and applications. Based on this analysis, check for adherence with the current changes. • Solution should support industry standards and comply to FIDO2. • During this process, user privacy and inclusion need to be mandated. • AI can play an effective role in improving the biometric process end-to-end. For instance, AI/ML algorithms could improve precision in capturing biometric traits (fingerprints, iris scan, facial features, etc.) by enabling real-time processing and error reduction during data collection. Machine Learning (ML) models learn and adapt to variations in biometric inputs (aging, lighting exposure, etc.) ensuring consistent performance across diverse environments and population.
Identity Evidence Validation	Refined criteria for validating identity evidence, incorporating advancements in document verification technologies. Adds new technologies, verifiable credentials, better biometrics	• As threats continuously evolve, ensuring better security makes identity verification a key factor in preventing any type of loss to a financial institution. In this context, incorporating the latest NIST changes to strengthen identity validation becomes significant. • Identify, document, and analyze, current list of accepted documents, verification policies for both physical and digital evidence verification process based on the environment and system in question. • This can be achieved by use of new technologies including AI/ML, verifiable credentials and better biometrics in the validation process while ensuring privacy. • AI/ML algorithms could be used to validate user identity using context-based patterns, biometric data and contextual signals along with enabling real-time, high assurance verification for sensitive service desk operations. The main aim should be to remove the risk of impersonation and unauthorized access, enhancing security and trust.
Fraud Detection	Enhanced measures to detect and prevent identity fraud during the proofing process.	• For financial institution fraud detection is paramount to prevent any form of loss. Having efficient identity validation, proofing and monitoring helps in preventing fraudulent access. • Mandate real-time liveness detection and anti-deepfake technologies. • Secure the privileged accounts, non-human, all types of admin accounts in a Credential Vault or Hardware Security Module (HSM) to ensure tamper-proof protection and reduce the risk of credential misuse as a part of fraud prevention. • Application of JIT, fine-grained access, zero trust adhering to least privilege will help in minimizing overprivileged access and reducing exposure to fraud from internal and external threats. • Conditional Access Policies with dynamic context authentication (including Device, IP, location, etc.). implementation helps prevent fraud detection. • Monitor logs for any suspicious activity and immediately block access in case of any risk or suspicion. • Leverage AI/ML-based Risk Assessment to proactively detect and respond to suspicious activities.

Authentication & Authenticator Management (SP 800-63B)

SP 800-63B introduces following key changes to authentication mechanisms and management:

Areas / Guideline / Framework	What's Changing?	How could this be addressed?
Phishing-Resistant Authentication	Stronger emphasis on phishing-resistant authentication methods, such as FIDO2 protocols.	• Verify if Authentication Assurance Level and If not already implemented, analyze & mandate the implementation of AAL2+ level • Review authentication methods and policies to consider passwordless options like passkeys, biometrics, and cryptographic authenticators (e.g., FIDO2, hardware keys). • Strengthen verifier impersonation resistance to ensure mutual trust and alignment with NIST Aug 2025 updates.
Password Guidelines	Updated recommendations for password policies, moving away from arbitrary complexity rules towards more user-friendly and secure approaches.	• tThis can be achieved by analyzing and overhauling password policies. Analyze current password policies for complexity and simplify them. • Remove outdated complexity requirements, eliminate the use of Knowledge-Based Authentication (KBA), avoid encouraging common or weak passwords, and screen for known password breaches. Favor long passphrases and remove forced password changes unless a risk-based justification exists, in line with NIST updates.
Multi-Factor Authentication (MFA)	Expanded guidance on implementing and managing MFA, including considerations for different types of authenticators.	• Review current Authentication and MFA Mechanism and based on the analysis on current conditional access policies, introduce tighter controls (e.g., session timeouts, persistent browser restrictions). • Insecure MFA methods like SMS and OTPs should be phased out in favor of stronger options such as biometrics and passkeys.
Authenticator Lifecycle Management (ALM)	Improved guidelines for managing the entire lifecycle of authenticators, from issuance to revocation.	• Review current Authentication, MFA, and Authentication lifecycle management. Ensure analysis of all the types of authenticators currently in use for its lifecycle management process. • Phishing-resistant MFA at AAL2+ / passkeys should be mandated.

Federation & Assertions (SP 800-63C)

SP 800-63C directs following updates in federated identity management:

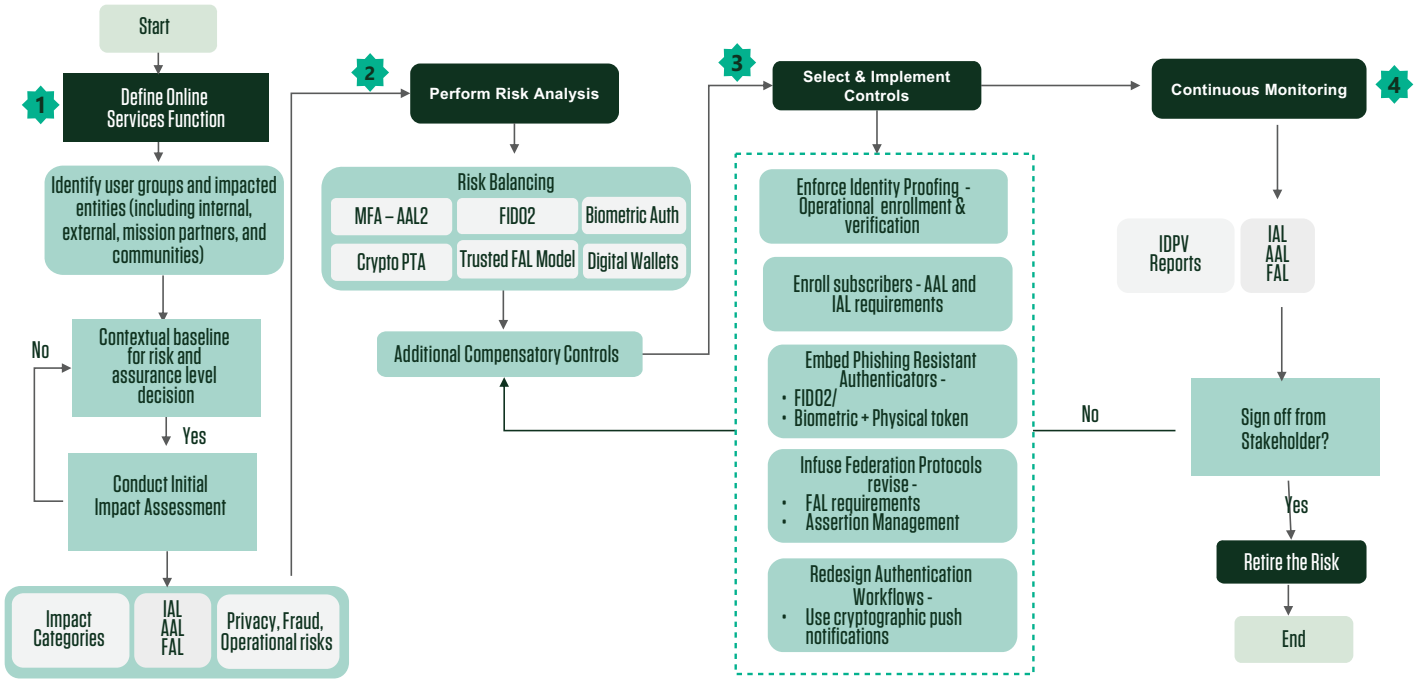
Areas / Guideline / Framework	What's Changing?	How could this be addressed?
Federation Protocols	Federation protocols have been updated to reflect current best practices and emerging standards. The update also clarifies FAL requirements, especially around proof-of-possession for assertions at FAL2 and FAL3. Federated logins must use direct cryptographic authentication.	• Analyze current assertions to check whether signed assertions are used alongside bearer assertions and verify support for endpoint validation and proof-of-possession, as these are now mandatory. • Check the currently implemented Federation Assurance Level (FAL) and ensure assertions are encrypted and replay resistant. • Based on findings, plan to implement refined Federation Assurance Level (FAL1–FAL3) with stronger replay protection. • As user consent and privacy is to be ensured, assess if user consent is explicitly captured and evaluate the number of shared identity attributes - emphasizing minimal attribute sharing per updated privacy standards.
Assertion Security	Enhanced measures to secure assertions and prevent common attacks in federated environments.	• Analyze the current assertion and check for adoption, assertion security compliance by federated partners.
Privacy in Federation	Enhanced measures to secure assertions and prevent common attacks in federated environments.	• Ensure assertions include timestamps, audience restrictions, and session binding.
Interoperability	Improved guidance on achieving interoperability between different identity providers and relying parties.	• Analyze all the IDPs in the environment and validate federation flows and ensure assertion integrity is mandated. • Adopt federation brokers or identity orchestration platforms to manage multiple IDPs.

Artificial Intelligence and Machine Learning in Identity Systems

- For the first time, SP 800-63-4 provides guidance concerning AI and ML integration:
  - AI-driven proofing and detection: Recommends responsible, explainable AI for document authenticity checks, biometrics, and risk flags.
  - Bias mitigation: Procedures for testing and minimizing bias in ML-based identity proofing (crucial for equity and legal compliance).
  - Monitoring and transparency: Requires detailed documentation and audits of AI/ML models influencing identity outcomes, with clear disclosure to affected individuals where appropriate.

How Infosys' solution can help adopt NIST SP 800-63-4?

Infosys has a comprehensive solution approach to meet business goals in relation to adoption of NIST SP 800-63-4. Below is a quick view of recommended flow to initiate the journey:



Conclusion

NIST SP 800-63 Revision 4 provides a structured framework for Digital Identity, Authentication and Federation. It ensures that users accessing enterprise systems do so through a trusted, standardized identity process by following identity proofing, credential management, federation and assertions, and assurance levels for authentication and federation.

The organization needs to analyze and assess identity and access management gaps within the environment and define matrices and policies based on each associated scenario. Based on the gaps, organizations must start analyzing and creating an implementation plan to remediate the gaps related to Identity and Access Management systems based on NIST guidelines.

Glossary

Acronym	Full Form
AAL	Authenticator Assurance level
AI/ML	Artificial Intelligence/Machine Learning
ALM	Authentication Lifecycle Management
CSF	Cybersecurity Framework
FAL	Federation Assurance level
HSM	Hardware Security Module
IAL	Identity Assurance Level
IAM	Identity and Access Management
IDP	Identity Provider
IDP	Identity Provider
KBA	Knowledge based Authentication
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
NIST-CSF	National Institute of Standards and Technology (NIST) Cybersecurity Framework
NIST SP	NIST Special Publication
OTP	One Time Password
RP	Relying Party

References

1. https://pages.nist.gov/800-63-4/sp800-63.html
2. https://pages.nist.gov/800-63-4/sp800-63a.html
3. https://pages.nist.gov/800-63-4/sp800-63b.html
4. https://pages.nist.gov/800-63-4/sp800-63c.html
5. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

About the Authors

Neeraj Mathpal
Enterprise Security Architect

Neeraj leads the consulting and solution architecture function for the Americas within the Infosys Cybersecurity practice and brings over 21 years of experience across diverse security domains. He is passionate about helping enterprises become cyber secure.

K. S. Viswanathan
Solution Architect, Identity and Access Management

Viswanathan has over 14 years of experience in cybersecurity, specializing in Identity and Access Management (IAM) capabilities and products. He is driven by the goal of helping enterprises strengthen their identity security posture and leads large-scale transformation programs across North America.

Supriyo Bhattacharya
Senior Consultant, Identity and Access Management

Supriyo is an accomplished Identity and Access Management (IAM) specialist with over 9 years of experience in designing, implementing, and optimizing enterprise-scale IAM solutions. He is recognized for driving secure digital identity strategies, enhancing user experience, and reducing operational risk through automation and zero-trust principles.

Atul Sharma
Principal Consultant, Identity and Access Management

Atul is an accomplished IAM Architect with 16+ years of specialized experience in IAM architecture and engineering. He brings proven expertise in designing and delivering end-to-end IAM solutions and maintains a forward-thinking approach to shaping the future of digital identity, exploring how AI/ML and agentic automation can transform access management and identity security governance.

For more information, contact askus@infosys.com

Infosys®
Navigate your next