Deloitte.

October 2021

FFIEC Guidance on Authentication and Access to Financial Institution Services and Systems

Deloitte Center for Regulatory Strategy, Americas

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Evolution of FFIEC guidance

On August 11, 2021, the Federal Financial Institutions Examination Council (FFIEC)[1], on behalf of its members, issued *Authentication and Access to Financial Institution Services and Systems Guidance (2021)* that provides financial institutions with examples of effective authentication and access risk management principles and practices for customers, employees, and third parties accessing digital banking services and information systems. The Guidance replaces the FFIEC-issued *Authentication in an Internet Banking Environment (2005)* and the *Supplement to Authentication in an Internet Banking Environment (2011).* The guidance acknowledges significant risks associated with the cybersecurity threat landscape that reinforce the need for financial institutions to effectively authenticate users and customers to protect information systems, accounts, and data.

Authentication in an Electronic Banking Environment
FIL-103-2005

- Provide sufficient protection for Internet-based financial services.
- **Risk assessments** should provide the basis for determining an effective authentication strategy according to the risks associated with the various services available to on-line customers.
- **Customer awareness and education** should continue to be emphasized because they are effective deterrents to the on-line theft of assets and sensitive information.

Authentication in an Electronic Banking Environment
FIL-50-2011

Institutions are expected to upgrade their controls for high-risk online transactions through:

- **Yearly risk assessments**;
- For consumer accounts, **layered security controls**;
- For business accounts, **layered security controls** consistent with the increased level of risk posed by business accounts; and
- **More active consumer awareness and education** efforts.

Authentication and Access to Financial Institution Services and Systems
FIL-55-2021

In addition to the requirements around conducting risk assessments, implementing multi-factor authentication (MFA), and layered security, the latest guidance directs to:

- Establish the **principle of least privilege** while provisioning access and implement **monitoring, activity logging, and reporting** processes
- Ensure **secure credential and application programming interface (API)-based authentication**
- Establish security controls to **secure email systems and internet browsers**
- Establish secure processes for **customer call center and IT help desk operations** and **customer and user identity verification**

1 The Council consists of the following six voting members: a member of the Board of Governors of the Federal Reserve System; the Chairman of the Federal Deposit Insurance Corporation; the Director of the Consumer Financial Protection Bureau; the Comptroller of the Currency; the Chairman of the National Credit Union Administration; and the Chairman of the State Liaison Committee.

Key takeaways

Authentication and Access to Financial Institution Services and Systems

- Highlights the **current cybersecurity threat environment** including increased remote access by customers and users, and attacks that leverage compromised credentials; and mentions the risks arising from push payment capabilities.
- Recognizes the importance of the financial institution's **risk assessment to determine appropriate access and authentication practices** for the wide range of users accessing financial institution systems and services.
- Supports a financial institution's **adoption of layered security** and **underscores weaknesses in single-factor authentication**.
- Discusses how **MFA** or controls of equivalent strength can more effectively mitigate risks.
- Includes **examples of authentication controls**, and **a list of government and industry resources** and references to assist financial institutions with authentication and access management

Who does this guidance apply to?

The **'Authentication and Access to Financial Institution Services and Systems'** guidance applies to FIs if the FI falls under one of the below mentioned categories:

Financial institutions offering Internet-based products and services

Third parties that act on behalf of financial institutions and provide accessed information systems and authentication controls

What do financial institutions need to be mindful of in the 2021 guidance?

Authentication and Access to Financial Institution Services and Systems Summary (1 of 3)

The below section outlines additional requirements that financial institutions must consider in addition to prior FFIEC 2011 compliance efforts.

	Section	Is this a new requirement?	Key Requirements & Considerations (FFIEC 2021)
1	**Threat Landscape**	No – Present in 2011 guidance	• Emphasis on considering **advances in technologies and control frameworks** while performing risk assessment and selecting authentication controls. • Along with MFA which was mentioned in the 2011 guidance, the 2021 guidance recommends implementation of **network segmentation and least privilege user access.**
2	**Risk Assessment**	No – Present in 2011 guidance	• The Guidance advises institutions to conduct **periodic risk assessments (at minimum annually)** • Emphasis has been laid on **integrated, enterprise-wide approach to risk assessment.** For example**, holistic risk assessment** including but not limited to fraud research, customer service, and cybersecurity can provide correlated data and actionable insights. • Recommended risk assessment practices include - inventory of information systems, visibility of high-risk users and transactions, threat identification, control assessments, etc.
3	**Layered Security**	No – Present in 2011 guidance	• The **principle of least privilege** provisioning has been explicitly called out under layered security • As per the latest guidance, controls in the layered security program must be applied **commensurate with the increasing risk level** associated with a transaction or access to an information system. • The guidance has underscored the implementation of **multiple preventative, detective, and corrective controls.** Although the specific controls have not been mentioned, those might include data protection, vulnerability and patch management, network security, continuous monitoring, etc.
4	**Multi-Factor Authentication as Part of Layered Security**	No – Present in 2011 guidance	• The guidance advises all financial institutions to assess whether **residual risk associated with authentication mechanisms** is **consistent with the financial institution's risk appetite** and security policies.

Authentication and Access to Financial Institution Services and Systems Summary (2 of 3)

	Section	Is this a new requirement?	Key Requirements & Considerations
5	**Monitoring, Logging, and Reporting**	No – Present in 2011 guidance	• While 2011 Guidance referred to identifying suspicious activities or transactions, the latest Guidance recommends **increased monitoring scope** to determine attempted or realized unauthorized access to information systems and accounts. • In addition, Organizations should **facilitate timely response and investigation** of unusual or unauthorized activity.
6	**Email Systems and Internet Browsers**	**Yes**	• The Guidance strongly advises financial institutions to establish risk management practices to protect email systems and internet browsers • The controls may include **secure configurations, MFA or equivalent access techniques, conducting awareness programs, patching vulnerabilities,** and implementing software vendor and service provider recommended controls for outsourced services
7	**Call Center and IT Help Desk Authentication**	**Yes**	• Per the latest guidance, financial institutions are directed to **prevent social engineering and other attacks** for customer call center and IT help desk operations • The controls may include **performing comprehensive risk assessment, identifying emerging threats, setting secure processes, employee training, and establishing effective controls**
7	**Data Aggregators and Other Customer-Permissioned Entities (CPEs)**	**Yes**	• The Guidance advises financial institutions to assess the risks and deploy **effective mitigating controls for credential and API-based authentication** accordingly, especially when CPEs access a financial institution's information systems and customer information.

Authentication and Access to Financial Institution Services and Systems Summary (3 of 3)

	Section	Is this a new requirement?	Key Requirements & Considerations
7	**User and Customer Awareness and Education**	No – Present in 2011 guidance	• The latest version of the guidance includes **examples of program elements** (e.g., legitimacy of communications from organizations, controls the financial institution offers, communication mechanisms, legal and other rights and protections, contacts) to be considered in developing a customer awareness program.
8	**Customer and User Identity Verification**	**Yes**	• Financial institutions are directed to **use reliable identity verification methods** while creating new customer accounts. • All financial institutions are required by the USA PATRIOT Act regulations to **establish a process to verify customer identity** when establishing a customer account.

Mapping FFIEC 2021 Guidance to NIST CSF (1 of 2)

The FFIEC Guidance refers to the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) standards. Key sections of the FFIEC Guidance are mapped to the categories of NIST CSF standard to help achieve compliance.

NIST CSF Category	Threat Landscape 1	Risk Assessment 2	Layered Security 3	MFA as Part of Layered Security 4	Monitoring, Logging, and Reporting 5	Email Systems and Internet Browsers 6	Call Center and IT Help Desk Authentication 7	Data Aggregators and Other CPE 8	User and Customer Awareness and Education 9	Customer and User Identity Verification 10
Asset Management		✓								
Business Environment										
Governance		✓								
Risk Assessment		✓					✓	✓		
Risk Management Strategy		✓					✓	✓		
Supply Chain Risk Management		✓								
Access Control	✓		✓	✓			✓	✓		✓
Awareness and Training							✓		✓	
Data Security			✓			✓				
IP Protection Processes and Procedures		✓	✓			✓				
Maintenance										
Protective Technology	✓		✓			✓				

Legend Identify Protect Detect Respond Recover

Mapping FFIEC 2021 Guidance to NIST CSF (2 of 2)

The FFIEC Guidance refers to the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) standards. Key sections of the FFIEC Guidance are mapped to the Categories of NIST CSF standard to help achieve compliance.

NIST CSF Category	Threat Landscape 1	Risk Assessment 2	Layered Security 3	MFA as Part of Layered Security 4	Monitoring, Logging, and Reporting 5	Email Systems and Internet Browsers 6	Call Center and IT Help Desk Authentication 7	Data Aggregators and Other CPE 8	User and Customer Awareness and Education 9	Customer and User Identity Verification 10
Anomalies & Events			✓		✓					
Security Continuous Monitoring	✓		✓		✓					
Detection Processes	✓		✓		✓					
Response Planning	✓				✓					
Communications					✓					
Analysis					✓					
Mitigation					✓					
Improvements					✓				✓	
Recovery Planning	✓									
Improvements									✓	
Communications										

Legend Identify Protect Detect Respond Recover

Next steps: Achieving compliance

Implementing the following phased approach can help financial institutions achieve compliance with guidance and close out significant gaps.

Do Now

- ✓ Understand FFIEC 2021 guidelines, contextualize the requirements with respect to existing risk and controls framework
- ✓ Conduct a gap analysis of the following capabilities against the FFIEC 2021 requirements:
  - Threat landscape, risk assessment, layered security, authentication (including MFA), monitoring and logging, email systems and browsers, call center and IT help desk authentication, data aggregators and other CPEs, user and customer awareness and education, customer and user identity verification
- ✓ Develop a gap-remediation strategy and roadmap

Do Next

- ✓ Implement prioritized gap remediation recommendations, which may or may not include:
  - Update risk assessment programs to incorporate expanded scope and increase frequency of risk assessments
  - Implement or improve layered security controls such as access controls, data protection controls, vulnerability and patch management processes, network security controls, continuous monitoring mechanisms, etc.
  - Expand the scope of logging, monitoring, and suspicious activity detection
  - Enhance visibility of critical assets, high-risk users (including customers and vendors), high-risk transactions, and cyber threats
- ✓ Improve existing security awareness programs and implement security awareness and training programs for customers and users
- ✓ Automate select business as usual (BAU) activities to achieve efficiency gains

Do Later

- ✓ Adopt new technologies for layered security (limit access to certain automated command features, establish dual controls for certain critical systems or administrative changes, etc.)
- ✓ Refine existing threat and vulnerability programs based on evolution of new technologies
- ✓ Build or upgrade existing cyber threat intelligence programs, as well as forensic and analytical capabilities
- ✓ Tighter integration with existing infrastructure and future capabilities

Appendix

Appendix – Example of practices and controls (1/2)

Below are examples of practices or controls related to access management, authentication, and supporting controls. These are listed in the appendix of the guidance.

Authentication Solutions

- Device-based Public Key Infrastructure (PKI) Authentication
- One-time Passwords (OTP)
- Behavioral Biometrics Software
- Device Identification and Enrollment

Password Controls

- Password Protection
- Unique Passwords
- Password Strength
- Prohibited Password Lists

Access and Transaction Controls

- Account Maintenance Controls
- Transaction Value, Frequency, and Timing Controls
- Rate Limit on Log-in Attempts
- Incorrect Log-in Attempts
- Application Timeouts
- Automatic Suspension or De-provisioning of User Credentials
- Notification to Security Administrators of Change in User Status

Customer Call Centers and IT Help Desks Controls

- Enhanced Authentication for Credential Reset
- Identify Unauthorized Access Attempts
- Lost, Stolen, or Changed Information and Devices
- Training on Password Reset Process

Customer Controls

- Positive Pay and Other Transaction Blocks
- Transaction Alerts
- Business Customer - System Administrators
- Dual Control Transactions

Transaction Logging and Monitoring Controls

- Transaction and Audit Logs
- Fraud and Anomaly Detection Monitoring
- Suspicious Behavior Monitoring
- Fraud Response Policies
- Monitoring and Reporting of Unauthorized Access by Third Parties

Appendix – Example of practices and controls (2/2)

Below are examples of practices or controls related to access management, authentication, and supporting controls. These are listed in the appendix of the guidance.

System Access Controls for Users

- Access Approval Policies
- Least Privilege Access Provisioning
- Single Sign-On Capability
- Service Accounts
- User Communication and Training

Privileged User Controls

- Change Defaults
- Dedicated Devices or Accounts
- Log and Alert
- Log Access
- Periodic Review of Privileged User Activity
- Dual Controls for Certain Critical Systems or Administrative Changes
- Enhanced Authentication for System and Software Updates

System and Network Design and Architecture Controls

- Endpoint / Device Authentication
- Device Blocking or Network Indicators
- Network Segmentation
- Remote Access Software Controls
- Configure and Update Security Devices and Software
- Limit Access to Certain Automated Command Features
- Transport Layer Security
- Digital Certificates
- Device Credentials

Email Systems Controls

- Service Provider Recommended Configuration
- Patch Management
- Layered Security and MFA Consideration
- Monitoring
- Anti-Phishing Controls
- External Email Alerts
- User Education
- Testing and Training Users

Internet Browser Controls

- Use of Current Updated Browsers
- Blocks on Certain Browser Features
- Blocking of Certain Scripting Languages
- Limit User Access
- Domain Filtering

Contacts

Irena Gecas-McCarthy
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
igecasmccarthy@deloitte.com
+1 212 436 5316

Julie Bernard
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
juliebernard@deloitte.com
+1 978 239 6263

Mark Nicholson
Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
manicholson@deloitte.com
+1 201 499 0586

Kedar Barve
Managing Director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
kbarve@deloitte.com
+1 732 500 6294

Anish Srivastava
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
anissrivastava@deloitte.com
+1 817 307 8354

Maniak Shome
Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
mshome@deloitte.com
+1 470 434 5181

Deloitte.

About the Deloitte Center for Regulatory Strategy
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experience executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.

www.deloite.com/us/centerregulatorystrategies