Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • www.ffiec.gov

Authentication and Access to Financial Institution Services and Systems

Introduction

The Federal Financial Institutions Examination Council (FFIEC) on behalf of its members[1] is issuing this guidance titled *Authentication and Access to Financial Institution Services and Systems* (the Guidance) to provide financial institutions with examples of effective risk management principles and practices for access and authentication. These principles and practices address business and consumer customers, employees, and third parties that access digital banking services[2] and financial institution 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)*, which provided risk management practices for financial institutions offering Internet-based products and services. This Guidance acknowledges significant risks associated with the cybersecurity threat landscape that reinforce the need for financial institutions to effectively authenticate users and customers[3] to protect information systems, accounts, and data. The Guidance also recognizes that authentication considerations have extended beyond customers and include employees, third parties, and system-to-system communications.

This Guidance highlights risk management practices that support oversight of identification, authentication, and access solutions as part of an institution's information security program. Periodic risk assessments inform financial institution management's decisions about authentication solutions and other controls that are deployed to mitigate identified risks. When a risk assessment indicates that single-factor authentication with layered security is inadequate, multi-factor authentication (MFA) or controls of equivalent strength, combined with other layered security controls, can more effectively mitigate risks associated with authentication.

Financial institutions are subject to various safety and soundness standards, such as the standard to have internal controls and information systems that are appropriate to the institution's size and complexity and the nature, scope, and risk of its activities.[4] Applying the principles and

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

[2] Digital banking refers to any banking service or platform that utilizes Internet or mobile cellular network communications for providing customers with banking services or transactions.

[3] For purposes of this Guidance only, the terms "users" and "customers" are defined in section 1 of this Guidance.

[4] See, for example, Interagency Guidelines Establishing Standards for Safety and Soundness: 12 CFR 30, Appendix A, II(A) (OCC); 12 CFR 208, Appendix D-1, II(A) (FRB); and 12 CFR 364, Appendix A, II(A) (FDIC). See also 12 CFR § 741.3 (NCUA).

practices in this Guidance, as appropriate to a financial institution's risk profile, can support alignment with such safety and soundness standards.

An effective authentication program also can support alignment with the *Interagency Guidelines Establishing Information Security Standards*[5] and with other laws and regulations. For example, a financial institution's authentication program can support compliance with consumer financial protection laws, and with laws that address Customer Identification Program (CIP) and Customer Due Diligence (CDD) requirements, identity theft prevention,[6] and the enforceability of electronic agreements. This Guidance does not interpret or establish a compliance standard for these laws or impose any new regulatory requirements on financial institutions.

This Guidance is not intended to serve as a comprehensive framework for identity and access management programs and does not endorse any specific information security framework or standard. This Guidance is relevant whether the financial institution or a third party, on behalf of the financial institution, provides the accessed information systems and authentication controls.

Management may refer to the appropriate FFIEC member issuances and resources referenced in the "Additional Resources" section of this Guidance to learn more about sound authentication and information technology risk management practices. This Guidance also contains references to other authentication risk management resources, including publications from the National Institute of Standards and Technology (NIST), National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Center for Internet Security (CIS), and other public and private industry organizations. Updates to these resources can assist financial institution management in evaluating new authentication threats and control practices.

Section 1. Highlights of Guidance

This Guidance sets forth risk management principles and practices that can support a financial institution's authentication of (a) users accessing financial institution information systems, including employees, board members, third parties, service accounts, applications, and devices (collectively, users) and (b) consumer and business customers (collectively, customers)[7] authorized to access digital banking services. The application of these principles and practices may vary at financial institutions based on their respective operational and technological complexity, risk assessments, and risk appetites and tolerances.

---

[5] The Interagency Guidelines Establishing Information Security Standards, which implement section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801, require banks and other financial institutions to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship. Credit unions are subject to a similar rule. 12 CFR 30, Appendix B (OCC); 12 CFR 208, Appendix D-2 and 225, Appendix F (FRB); 12 CFR 364, Appendix B (FDIC); and 12 CFR 748, Appendix A (NCUA). These principles also are consistent with resources provided by the FFIEC members, and the "Joint Statement on Heightened Cybersecurity Risk" issued by the OCC and FDIC.

[6] See, for example, the Identity Theft Red Flags Rule. 12 CFR § 334.90 (FDIC); 12 CFR 222, subpart J (FRB); and 12 CFR 41, subpart J (OCC).

[7] For purposes of this Guidance only, the term "customers" includes credit union members.

Topics of this Guidance include:

- Conducting a risk assessment for access and authentication to digital banking and information systems.
- Identifying all users and customers for which authentication and access controls are needed, and identifying those users and customers who may warrant enhanced authentication controls, such as MFA.
- Periodically evaluating the effectiveness of user and customer authentication controls.
- Implementing layered security to protect against unauthorized access.
- Monitoring, logging, and reporting of activities to identify and track unauthorized access.
- Identifying risks from, and implementing mitigating controls for, email systems, Internet access, customer call centers, and internal IT help desks.
- Identifying risks from, and implementing mitigating controls for, a customer-permissioned entity's access to a financial institution's information systems.
- Maintaining awareness and education programs on authentication risks for users and customers.
- Verifying the identity of users and customers.

Section 2. Threat Landscape

The system entry or access points (known as the attack surface) where an attacker can compromise a financial institution have expanded with the evolution of new technologies and broadly-used remote access points. For example, the number of digital banking services and information system access points has expanded with mobile computing, smart phone applications, "bring your own" devices, voice-activated capabilities, and cellular communications. These technologies and access points provide attackers with more opportunities to obtain unauthorized access, commit fraud and account takeover, or exfiltrate data. Authentication risks may arise from: (a) expanded remote access to information systems; (b) the types of devices and third parties accessing information systems; (c) the use of application programming interfaces (APIs); and (d) financial institutions' increased connectivity to third parties, such as cloud service providers.

Data breaches at financial institutions, their service providers, and nonbanks, such as credit bureaus, have exposed information and credentials of customers and employees. Attackers use technologies, such as automated password cracking tools, and these compromised credentials in their attacks against financial institutions. In addition, older or unsupported information systems may be especially vulnerable to attacks because security patches and upgrades for authentication controls can be more difficult to obtain.

These types of attacks demonstrate that certain authentication controls, previously shown effective, no longer provide sufficient defense against evolving and increasingly sophisticated methods of attack. In particular, malicious activity resulting in compromise of customer and user accounts and information system security has shown that single-factor authentication, either alone or in combination with layered security, is inadequate in many situations.

While the financial sector continues to expand the number of systems and services that require effective authentication, advances in technologies and control frameworks can support financial institution management's risk assessment and selection of authentication controls. For example, some authentication controls use out-of-band communication and encryption protocols to support secure authentication. Various standard-setting organizations and other cybersecurity resources have identified MFA, in conjunction with other layered security controls, to be an effective practice to secure against financial loss and data compromise caused by various threats.[8] For example, MFA, when combined with network segmentation and least privilege user access, can assist in mitigating the risk of unauthorized access that can result in a threat actor changing system configurations, exfiltrating data, or moving laterally within a network or system.

Section 3. Risk Assessment

A risk assessment[9] evaluates risks, threats, vulnerabilities, and controls associated with access and authentication, and supports decisions regarding authentication techniques and access management practices.[10] Risk assessments conducted prior to implementing a new financial service, such as a faster payment product, as well as periodic risk assessments, have been shown to be effective in identifying reasonably foreseeable risks.[11] A non-current risk assessment may result in unidentified risks or insufficient controls.

An integrated, enterprise-wide approach to a risk assessment includes inputs from a range of business functions or units. For example, fraud research, customer service, and cybersecurity can provide data and perspectives to enhance the risk assessment. Data from these business functions, as well as from customer reports of attempted and actual fraud, may yield useful information for identifying emerging authentication threats. Moreover, data from actual fraud events may enable financial institutions to identify certain authentication controls that are ineffective or degraded.

Examples of effective risk assessment practices include:

- *Inventory of Information Systems*. Inventory all information systems and their components, such as the hardware, operating systems, applications, infrastructure devices, APIs, data, and other assets, that require authentication and access controls. This inventory includes information systems provided by the financial institution's third parties, such as cloud service providers.

[8] See for example, NIST Special Publication 800-63B, Digital Identity Guidelines - Selecting Assurance Levels; CISA and Multi-State Information Sharing and Analysis Center (MS-ISAC), "Joint Ransomware Guide" (September 2020); NSA, "Top Ten Cybersecurity Mitigation Strategies" (March 2018).
[9] While this Guidance refers to a single risk assessment, a financial institution may have more than one risk assessment to evaluate threats and controls at different levels, such as the enterprise, system, or application levels, consistent with the financial institution's internal practices and policies.
[10] The *Interagency Guidelines Establishing Information Security Standards,* paragraph III.B (*Assess Risk*) and paragraph III.C (*Manage and Control Risk*) states that a financial institution subject to the Guidelines shall assess risk and shall consider among other things whether access controls on customer information systems, encryption controls, and monitoring systems are appropriate. For more information on risk assessments, see *FFIEC IT Examination Handbook*, "Information Security" booklet; and FFIEC Cybersecurity Assessment Tool. See NIST Special Publication 800-30, Revision 1 – "Guide for Conducting Risk Assessments" (2012).
[11] *FFIEC IT Examination Handbook*, "Management" booklet, section III, IT Risk Management.

- *Inventory of Digital Banking Services and Customers*. Inventory digital banking services, customers, and transactions that may warrant authentication and access controls. This includes such elements as: customer types (e.g., business or consumer), transactional capabilities (e.g., bill payment, wire transfer, loan origination), customer information accessed, and transaction volumes. Some digital banking services may have unique risk profiles. For example, financial institutions may benefit from considering risks arising from digital payment services that have shorter processing windows, push-payment capabilities, and limited fraud management functionality.[12]

- *Identify Customers Engaged in High-Risk Transactions*. Identify digital banking customers engaged in transactions that present higher risk of financial loss or potential breach of information for which enhanced authentication controls are warranted. [13] Elements considered in identifying high-risk transactions have included the dollar amount and volume of transactions, the sensitivity and amount of information accessed, the irrevocability of the transaction, and the likelihood and impact of fraud.

- *Identify Users.* Identify all users, including employees, service accounts,[14] and users at third parties, that access financial institution information systems and data. Considerations have included the functionality, criticality, and associated risk of information systems and data, and user access rights or permissions.

- *High-Risk User Identification*. Identify users who represent a high risk and for which enhanced authentication controls are warranted to protect information systems. Elements considered when identifying high-risk users have included: access to critical systems and data; privileged users,[15] including security administrators; remote access to information systems; and key positions such as senior management. For purposes of this Guidance, this subset of users that warrant enhanced controls are referred to as "high-risk users."

- *Threat Identification*. Identify threats with reasonable probability of impacting financial institution information systems, data, and user and customer accounts. Common threats include, but are not limited to, malware including ransomware, man-in-the middle (MIM) attacks, credential abuses, and phishing attacks. Threat identification typically includes intelligence from Information Sharing and Analysis Organizations,[16] and a review of actual or attempted incidents of security breaches, identity theft, or fraud experienced by the institution or the financial industry. Refer to NIST and other resources set forth in the

[12] In traditional payment transfers, the entity receiving funds initiates a transfer to pull funds from a customer account using payment credentials. In contrast, some payment products—particularly newer faster products—allow paying customers to log into their accounts and initiate a credit "push" of funds to another account.
[13] Financial institution management may decide to apply enhanced authentication more broadly across the institution's customer base, regardless of the relative risks associated with different customers' transactions.
[14] A service account is a "dedicated account with escalated privileges used for running applications and other processes. Service accounts may also be created just to own data and configuration files. They are not intended to be used by people, except for performing administrative operations." Glossary, CIS Controls, version 8.
[15] NIST SP 800-53 Rev. 5 defines a "privileged user" as a "user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform."
[16] These organizations include the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the United States Computer Emergency Readiness Team (US-CERT) of CISA.

"Additional Resources" section of this Guidance for additional threat identification and mitigation information.[17]

- *Controls Assessment*. Initially and periodically assess the design and effectiveness of access and authentication controls employed, including the availability of more advanced security options and configuration settings. Based on control assessments, residual risk is considered for acceptance or additional corrective action according to internal policies that define risk appetite and tolerance. Examples of assessment areas include source code and supply chain management controls for authentication factors, and service level agreements (SLAs) with measurement and reporting controls for outsourced authentication services.

Section 4. Layered Security

Layered security incorporates multiple preventative, detective, and corrective controls, and is designed to compensate for potential weaknesses in any one control.[18] Consistent with the assessed level of risk, the application of these controls can mitigate inherent risk associated with, and protect against unauthorized access to, information systems and digital banking services. Layered security controls can include, but are not limited to, MFA, user time-out, system hardening, network segmentation, monitoring processes, and transaction amount limits. Layered security controls also can include assigning users' access rights to information systems based on the principle of least privilege provisioning. Refer to the Appendix and the "Additional Resources" section of this Guidance for further examples and information regarding authentication and access controls.

Relying only on a single control or authentication solution can increase risk to information systems and digital banking services. In a layered security approach, authentication controls are applied commensurate with the increasing risk level associated with a transaction or access to an information system. Authentication controls with increased strength have been shown to be effective for customers and users engaged in high-risk transactions and activities, for example, when a customer initiates a payment transaction or when a privileged user accesses an information system.

Section 5. Multi-Factor Authentication as Part of Layered Security

Attacks against systems and users protected with single-factor authentication often lead to unauthorized access resulting in data theft or destruction, adverse impacts from ransomware, customer account fraud, and identity theft. Accordingly, use of single-factor authentication as the only control mechanism has shown to be inadequate against these threats. Furthermore,

[17] For example, see NIST SP 800-63B - Digital Identity Guidelines – Authentication Lifecycle Management, section 8.1. The "Threats and Considerations" section contains a list of "Authenticator Threats" and "Mitigating Authenticator Threats."

[18] See *FFIEC IT Examination Handbook*, "Information Security" booklet, section II.C.15(c) ("Remote Access"), and section II.C.16 ("*Customer Remote Access to Financial Services*") for information about layered security.

single-factor authentication with layered security has shown to be inadequate for customers engaged in high-risk transactions and for high-risk users.[19]

When a financial institution management's risk assessment indicates that single-factor authentication with layered security is inadequate, MFA or controls of equivalent strength as part of layered security can more effectively mitigate risks. When selecting an authentication solution, such as MFA, effective risk assessment practices consider whether any residual risk associated with the authentication solution is consistent with the financial institution's risk appetite and security policies.[20]

MFA is defined by NIST as:

> *An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.*[21]

MFA factors may include memorized secrets, look-up secrets, out-of-band devices, one-time-password devices, biometrics identifiers, or cryptographic keys. The attributes, including usability, convenience, and strength, of various authentication factors can differ and each may exhibit different vulnerabilities which may be exploited. For example, certain MFA factors may be susceptible to MIM attacks, such as when a hacker intercepts a one-time security code sent to a customer.

The following are some considerations when evaluating or implementing MFA:

- For digital banking customers engaging in high-risk transactions, MFA solutions and other layered security controls may vary depending upon the different risks presented by various services and customer segments, such as business or consumer customers.

- For high-risk users, strong authentication, such as MFA solutions using hardware and cryptographic factors, can mitigate risks associated with unauthorized access to information systems. When cryptographic MFA solutions are used, cryptographic keys are stored securely and protected from attack, for example by storing keys in a hardware security module. For remote users, remote access software (e.g., virtual private network software) can be protected with MFA user credentials in order to improve the security of the encrypted access channel.

---

[19] See discussion regarding identifying high-risk scenarios in the "Risk Assessment" section of this Guidance.
[20] See *FFIEC IT Examination Handbook*, "Information Security" booklet, section I.B. "Responsibility and Accountability" for more information about the role of management conducting a risk assessment and acceptance of risk for certain activities.
[21] NIST SP 800-63-3, Appendix A – Definitions and Abbreviations. Definition of "Multi-factor Authentication." The NIST Digital Identity Guidelines also describe different types of multi-factor authentication solutions and their relative levels of security.

- The use of standards and controls can protect the integrity of authentication factors (e.g., tokens, keys, passwords, or passphrases) and communication channels (e.g., out-of-band devices, encrypted communications). Controls can include implementation of validated cryptographic tools to mitigate the risk of authenticator modification, replay, or bypass by a malicious actor.

Section 6. Monitoring, Logging, and Reporting

Monitoring, activity logging, and reporting processes and controls assist financial institution management in determining if attempted or realized unauthorized access to information systems and accounts has occurred. They also facilitate timely response and investigation of unusual or unauthorized activity. Transaction and audit logs assist with identification of unauthorized intrusion or suspicious internal activities, help reconstruct adverse events, and promote employee and user accountability. Refer to the Appendix and the "Additional Resources" section of this Guidance for examples of these controls.

Section 7. Email Systems and Internet Browsers

Users' email accounts and Internet browsers are common access points used by threat actors to gain unauthorized access, obtain or compromise sensitive data, or initiate fraud. These attacks frequently take advantage of misconfigured applications, operating systems, and unpatched vulnerabilities by using social engineering and phishing campaigns. Examples of risk management practices shown to be effective for a financial institution's email systems include implementing secure configurations, MFA or equivalent access techniques, continuing education of users, patching vulnerabilities, and the implementation of software vendor and service provider recommended controls for outsourced services. Examples of risk management practices shown to be effective for Internet browsers include blocking browser pop-ups and redirects and limiting the running of scripting languages. Refer to the Appendix and the "Additional Resources" section of this Guidance for examples of these controls.

Section 8. Call Center and IT Help Desk Authentication

Threat actors frequently have used social engineering and other techniques to deceive customer call center and IT help desk representatives into resetting passwords and other credentials, thereby granting threat actors access to information systems, user and customer accounts, or confidential information. A comprehensive risk assessment supports mitigation of this risk by identifying emerging threats, setting secure processes, employee training, and establishing effective controls for the customer call center and IT help desk operations. Refer to the Appendix and the "Additional Resources" section of this Guidance for examples of these controls.

Section 9. Data Aggregators and other Customer-Permissioned Entities

Data aggregators and other customer-permissioned entities (collectively, CPEs) provide data aggregation and other services to business and consumer customers.[22] CPEs access financial institutions' customer account information directly, or through a third or fourth party. CPEs typically use this accessed data to provide financial institutions' customers a variety of services, such as personal financial management, consumer lending, and payments facilitation. With credential-based access, the CPE obtains and, in some cases, retains the customer's credentials to access the institution's digital banking service on an ongoing basis. Alternatively, with API-based or token-based access, the CPE interfaces directly with the financial institution's information systems using authentication credentials provided by the financial institution.

A comprehensive risk management program includes an assessment of risks and effective mitigating controls for credential and API-based authentication when CPEs access a financial institution's information systems and customer information. For example, a financial institution may assess how the controls applicable to different types of CPE access compare to the controls applicable to customers when directly accessing its digital banking service.

Section 10. User and Customer Awareness and Education

A comprehensive customer awareness program educates customers about a range of authentication risks and other security considerations when using digital banking services. The customer awareness program can complement the layered security controls implemented to protect customers and can lower access and authentication risks. Failure to update customer awareness programs and resources to reflect changes in risks, such as the introduction of a faster payments service, has been shown to cause such programs to become ineffective over time. Any related marketing that is inconsistent with the description of security risks in customer awareness programs could raise legal compliance risks.

In developing a customer awareness program, management may consider the following examples of program elements:

- An explanation of how customers can determine the legitimacy of communications from the financial institution, particularly communications that seek information that could be used to access the customer's account.
- An explanation of controls the financial institution offers that customers can use to mitigate risk, such as MFA.
- An explanation of communication mechanisms that customers may use to monitor account activity, such as transaction alerts.

[22] This Guidance does not address other risks or policy issues that may be associated with CPEs and data aggregation services, such as regulatory liability of parties for data breach. This Guidance should not be used to circumscribe or discourage customers' appropriate customer-permissioned access to their data through CPEs. For a discussion of risks and policy issues related to data aggregation services, see CFPB Advanced Notice of Proposed Rulemaking: Consumer Access to Financial Records, (October 22, 2020). For a discussion of different types of business arrangements associated with CPEs, see OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," (March 5, 2020).

- A listing of financial institution contacts that customers may use to report suspicious account activity or information security-related events.
- Educational information regarding prevalent external threats and methods used to illegally access accounts and account information, such as phishing, social engineering, mobile-based trojans, and business email compromise.
- An explanation of situations in which the institution uses enhanced authentication controls, such as call center contact or certain types of account activity like password reset.
- An explanation of the legal and other rights and protections a customer may have in the event of unauthorized access to an account, including protections under Regulation E.

For employees, board members, and other users accessing a financial institution's information systems, education can include training and testing programs on authentication-related scenarios such as phishing and social engineering.

Section 11. Customer and User Identity Verification

Reliable identity verification methods can help reduce risk when establishing new customer accounts and when access is first requested for new users of information systems. Identity verification can reduce the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Identity verification also occurs periodically thereafter based on risk factors, such as the granting of new authorities or access rights to a user within an information system. For customers, financial institutions are required by USA PATRIOT Act regulations to have a process to verify customer identity when establishing a customer account. Verification methods that detect fraudulent activities, such as synthetic identities[23] and instances of impersonation, have been shown to be effective in minimizing risk associated with identity verification. Reliable verification methods generally do not depend solely on knowledge-based questions to verify identity.

Financial institution management may consult their primary federal regulator or state supervisor, or FFIEC and Financial Crimes Enforcement Network guidance and resources for information about customer identity verification. Sources in the "Additional Resources" section of this Guidance include information on identity verification.

[23] Unlike typical identity theft fraud where a fraudster steals the identity of a real person and uses it to commit fraud, a synthetic identity is a completely fabricated identity that does not correspond to any actual person.

Appendix

The Appendix lists examples of practices or controls related to access management, authentication, and supporting controls. Practices and controls are part of the continuously evolving security landscape and the effectiveness of the listed practices and controls may change. This Appendix is provided as a reference and does not represent an all-inclusive list of practices or controls or characterize a comprehensive information security program. Additional control examples are contained in the resources listed in the "Additional Resources" section.

Authentication Solutions

- *Device-Based Public Key Infrastructure (PKI) Authentication.* PKI authentication solutions use private key/public key cryptography that is built into computers, smartphones, and other devices. A customer or employee uses a personal identification number, biometrics, or other identification methods on the device to trigger the encryption-based authentication process with the financial institution.[24]
- *One Time Passwords (OTP).* OTPs are generated using a specific hardware or software application installed on a mobile phone or other device and may be more secure than static passwords that are only changed at defined intervals.[25]
- *Behavioral Biometrics Software*. Software analyzes the behavioral biometrics or characteristics of a customer, such as the customer's interaction with a mobile phone or other access device, in order to authenticate the customer. Behavioral biometric analysis can include data such as the customer's finger swipes, taps, keystrokes, and mouse usage.
- *Device Identification and Enrollment*. Unique identifiers or characteristics of the customer's or user's device are identified and used to authenticate by obtaining a complex digital "fingerprint" of the device or by other secure identification techniques. Some device identifiers, such as device cookies, geo-location, and Internet Protocol (IP) address matching, are considered insecure and ineffective if used alone, but can be combined with other controls for additional protection.

Password Controls

- *Password Protection.* Passwords are stored in a manner that makes them resistant to attack and possible compromise. Protections are applied for static storage of passwords or the placement of passwords within an application or API. For example, passwords can be "salted" with a random or static value and hashed with a suitable hashing algorithm. This process is designed to mitigate the threat of a brute force or a pre-computed hash attack.
- *Unique Passwords.* Policies and standards address unique passwords for customers and users to minimize the risk of account takeover.

[24] See NIST Special Publication 800-63B, Digital Identity Guidelines - Authentication and Lifecycle Management for descriptions of "Single-Factor Cryptographic Devices" and "Multi-Factor Cryptographic Devices;" and NIST Special Publication 1800-17, Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers.

[25] See NIST Special Publication 800-63B, Digital Identity Guidelines - Authentication and Lifecycle Management for descriptions of "Single-Factor OTP Devices" and "Multi-Factor OTP Devices."

- *Password Strength.* Policies and standards address password strength, such as password length, defined character combinations, and the use of passphrases.[26] A passphrase is a series of words or other text that is generally longer than a traditional password.
- *Prohibited Password Lists.* Customers' or users' password choices are checked against databases of prohibited or weak passwords, including dictionary words, common passwords, and passwords associated with prior account or data breaches.

Access and Transaction Controls

- *Account Maintenance Controls*. Enhanced authentication controls are applied for account maintenance activities (e.g., changes to physical or email address, password, contact information, or enrolled devices) performed or requested by customers or users.
- *Transaction Value, Frequency, and Timing Controls.* Transaction controls, such as transaction value limits, restrictions on devices for adding payment recipients, limits on the number of transactions allowed per day, and allowable payment windows (i.e., permissible days and times during which transactions can be initiated) are applied for certain account and digital banking activities.
- *Rate Limit on Log-in Attempts.* Rate limits, which represent the number of log-in submissions over a set timeframe, are applied for correct and incorrect log-in attempts from the same user or from different users from the same IP address. These controls limit the overall volume of authentication requests and can slow potential attacks.
- *Incorrect Log-in Attempts.* Customers and users are locked out of accounts after a certain number of incorrect log-in attempts. Passwords are reset only after requiring strong authentication of the customer or user.
- *Application Timeouts*. Customers and users are re-authenticated after a period of inactivity within a service or a system.
- *Automatic Suspension or De-provisioning of User Credentials*. Policies and system controls are in place to de-provision or suspend access credentials after a certain period of account inactivity.
- *Notification to Security Administrators of Change in User Status*. System administrators are informed in a timely manner of changes (e.g., alteration, removal, or suspension) to user status.

Customer Call Centers and IT Help Desks Controls

- *Enhanced Authentication for Credential Reset*. Enhanced authentication controls are applied to customer and user credential resets, such as sending an OTP to a pre-established communication device; using an authenticator application to provide an OTP; biometric voice recognition; enabling secure video chat features to confirm identity; and call-backs to a pre-established phone number.

[26] See discussion of "Memorized Secret Authenticators" in NIST Special Publication 800-63B, Digital Identity Guidelines - Authentication and Lifecycle Management; and Section 3.7 – "Identification and Authentication - Authenticator Management" of NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

- *Identify Unauthorized Access Attempts*. Controls identify deviations from a customer's or user's usual geographic location or method of communication for the account, such as an Internet-based communication application or an unidentifiable phone number.
- *Lost, Stolen, or Changed Information and Devices.* Controls establish processes for handling lost, stolen, or changed information and devices, including changes to established phone numbers or carriers.
- *Training on Password Reset Process*. Call center personnel are trained on verification and authentication processes for password resets.

Customer Controls

- *Positive Pay and Other Transaction Blocks.* Positive pay,[27] debit blocks, and other techniques are available to business customers to monitor and control transactions on their accounts.
- *Transaction Alerts.* Automated alerts are sent to customers based on transaction size or risk parameters established by customers or the financial institution.
- *Business Customer - System Administrators.* Supplementary controls are available for a business customer's system administrators who are granted privileges to change digital banking configurations, such as the establishment of a new employee with transactional access on the account.
- *Dual Control Transactions.* Controls are available to business customers to require more than one employee to authorize and approve certain transactions.

Transaction Logging and Monitoring Controls

- *Transaction and Audit Logs*. Transaction and audit logs monitor and record system and account activity to identify unauthorized activities, detect intrusions, reconstruct events, and promote customer and user accountability.
- *Fraud and Anomaly Detection Monitoring.* Processes detect fraud and other anomalies, such as changes in user or customer behavior or transaction velocity and increases in login or account lockout activity. These processes also alert management to unauthorized access and/or fraud in a timely manner.
- *Suspicious Behavior Monitoring*. Processes monitor and report customer and user access, especially privileged and remote access users, for suspicious behavior.
- *Fraud Response Policies*. Response policies address situations where customer or user devices are identified as potentially compromised and where customers or users may be facilitating fraud.
- *Monitoring and Reporting of Unauthorized Access by Third Parties*. Processes are in place for third-party service providers to report, and the financial institution to log and monitor, unauthorized access to critical outsourced systems.

[27] "Positive pay" is a technique in which a business customer sends electronic files of information to the financial institution on all checks the business customer has issued. The financial institution compares this information against electronic information regarding checks presented for payment. If a check presented for payment is not included in the positive-pay information, the institution requests the business customer to make a pay/no pay decision.

System Access Controls for Users

- *Access Approval Policies*. Policies establish approval and documentation standards for defining users' authority to access financial institution information systems.
- *Least Privilege Access Provisioning*. User access is limited to those information systems and resources related to the user's job function or role. This can include limitation of users' access rights across multiple information systems.
- *Single Sign-On Capability*. Single sign-on capability is established for users to allow access to multiple internal information systems with a single authentication solution. Single sign-on capability can mitigate risk by reducing the number of passwords and credentials employees must manage and allow the application of strong authentication and risk monitoring to the single sign-on process.
- *Service Accounts.* Service accounts are inventoried, and employees or departments are assigned responsibility for managing service accounts according to the financial institution's password management and other security policies.[28]
- *User Communication and Training*. Users periodically receive authentication security awareness training.

Privileged User Controls

- *Change Defaults*. Default passwords and other credentials for privileged users or system, service, or administrative accounts are changed or disabled.
- *Dedicated Devices or Accounts*. Privileged users have dedicated devices or accounts for all privileged or administrative activities. The dedicated devices cannot access the Internet.[29]
- *Log and Alert.* Systems are configured to log and alert when a privileged user account is added or removed and when unsuccessful logins or other anomalous behavior occurs.[30]
- *Log Access.* Privileged user access is limited and defined between log-related privileges and other privileges. The logs of privileged user activity cannot be modified or deleted by the privileged user.[31]
- *Periodic Review of Privileged User Activity*. Staff independent of the privileged user's organization or business unit is alerted of, and periodically reviews, privileged user activity for anomalous behavior.
- *Dual Controls for Certain Critical Systems or Administrative Changes*. More than one privileged user at the financial institution must approve access to certain critical systems or certain requests for administrative changes.
- *Enhanced Authentication for System and Software Update*s. Privileged users are re-authenticated with MFA prior to making system configuration changes, uploading or updating software or firmware, or executing significant system processes.[32]

---

[28] Additional information regarding controls for service accounts users is available in the CIS Security Controls.
[29] Id.
[30] Id.
[31] NIST Special Publication 800-53 (Rev. 5), Control AU-9.4, Security and Privacy Controls for Federal Information Systems and Organizations.
[32] NIST Special Publication 800-160 Vol. 2 - Developing Cyber Resilient Systems: A Systems Security Engineering Approach.

System and Network Design and Architecture Controls

- *Endpoint / Device Authentication.* Controls are in place to ensure only authorized devices can connect to the financial institution's information systems, networks, or services.
- *Device Blocking or Network Indicators.* Connections to the financial institution's systems or servers are blocked based on devices, networks, or IP addresses known or suspected to be associated with fraudulent or malicious activities.
- *Network Segmentation*. Networks, systems, services, and data are physically and logically segmented based on the financial institution's asset classification and risk assessment.
- *Remote Access Software Controls*. Remote access software, which allows remote access to a user's computer or enterprise network or system, is disabled if it is not being used. If remote access software is used, controls to mitigate threats can include placing a firewall in front of systems that use remote access software, having remote users connect with a virtual private network (VPN) or other secure channel, and implementing strong passwords with MFA.[33] Software is updated periodically.
- *Configure and Update Security Devices and Software*. Network security devices and software are securely configured (e.g., implement firewall, router, or end-point security). Software and firmware are updated to address vulnerabilities.
- *Limit Access to Certain Automated Command Features.* Only authorized users and accounts have access to configuration management frameworks that utilize command-line shells. A user's access to these features is logged.
- *Transport Layer Security.* Transport Layer Security (TLS) protocols that utilize encryption and authentication to create private, secure channels between machines are implemented. TLS protocols are periodically updated to address vulnerabilities and implement additional security.
- *Digital Certificates*. An inventory of machines that utilize digital certificates is maintained, and digital certificates and the underlying protocols are continually updated to address emerging threats.[34]
- *Device Credentials*. Controls are in place to preserve the authenticity of machine (servers and clients) credentials in the form of digital keys and certificates, and to protect these credentials from compromise while in transit.

Email Systems Controls

- *Service Provider Recommended Configuration.* Email service vendor-recommended controls are implemented (e.g., MFA, anti-phishing, and anti-ransomware). Systems are monitored for unauthorized configuration changes.
- *Patch Management*. Email systems are updated and patched periodically, and the email system vendor is monitored for email system end-of-life.

[33] CISA Alert – "Microsoft Releases Security Update for Remote Desktop Services Vulnerability;" CIS, "Intel Insights: How to Disable Remote Desktop Protocol."
[34] NSA, Cybersecurity Information, "Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations."

- *Layered Security and MFA Consideration*. Layered security controls, to include the use of MFA or equivalent techniques, are applied for the email user population.
- *Monitoring*. Email systems are monitored to detect suspicious activity.
- *Anti-Phishing Controls*. Anti-phishing controls are applied to identify and block malicious emails and attachments. Specific controls may include:
    - "Watermarks" are in place to detect unauthorized emails;
    - Domain-based Message Authentication Reporting and Conformance (DMARC) policy and verification are enabled;
    - Macro scripts transmitted via email are disabled; and
    - Malicious email attachments are blocked and moved to a segregated environment.
- *External Email Alerts*. External email messages are labeled with a prominent notice or banner to alert the receiver that the email message comes from outside the financial institution.
- *User Education*. Users are educated on common email compromise tactics and techniques and offered ways to avoid or mitigate attacks.
- *Testing and Training Users*. Social engineering campaigns are administered to test users' comprehension of and adherence to security policies. User training techniques are adjusted based on test results.

Internet Browser Controls

- *Use of Current Updated Browsers.* Vendor-supported and management-approved Internet browsers are installed on systems and updated to the most current version in a timely manner**.**
- *Blocks on Certain Browser Features*. Internet browser pop-ups and redirects are blocked to protect against malware. Browser plug-ins and add-on applications are evaluated, with unnecessary plug-ins/applications disabled or removed.
- *Blocking of Certain Scripting Languages.* Scripting languages (i.e., JavaScript) that are run in Internet browsers are evaluated, and allowed or blocked. Cross-Site Scripting is an example where the attacker uses a scripting language to execute malware within a victim's browser.
- *Limit User Access.* Domains inconsistent with the financial institution's risk profile and policies are blocked.
- *Domain Filtering*. Domain Name System filtering services are implemented to prevent access to known malicious domains.[35] Institutions consider the use of a reputation service or similar technology for remaining domains.

[35] Additional information regarding controls for service accounts users is available in the CIS Security Controls.

Additional Resources

FFIEC	FFIEC IT Examination Handbook - Information Security Booklet FFIEC Statement - FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness FFIEC Cybersecurity Assessment Tool FFIEC Joint Statement - Destructive Malware FFIEC Joint Statement - Cyber Attacks Compromising Credentials FFIEC Joint Statement Security in a Cloud Computing Environment
FDIC and OCC	Joint Statement on Heightened Cybersecurity Risk
Conference of State Bank Supervisors (CSBS)	Ransomware Self-Assessment Tool
NIST	Special Publication 800-63 - Digital Identity Guidelines Cybersecurity Framework Computer Security Resource Center Glossary Special Publication 800-53, Revision 5 - Security and Privacy Controls for Federal Information Systems and Organizations Special Publication 800-177, Revision 1 - Trustworthy Email Special Publication 1800-16 - TLS Server Certificate Management Practice Guide Special Publication 800-46, Revision 2 - Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security Special Publication 800-30, Revision 1 - Guide for Conducting Risk Assessments Special Publication 800-207 - Zero Trust Architecture Special Publication 1800-17 – Multifactor Authentication for E-Commerce: Risk-Based, FIDO Universal Second Factor Implementations for Purchasers

CISA	CISA Cyber Essentials CISA INSIGHTS - Enhance Email & Web Security Security Tip (ST04-002) - Choosing and Protecting Passwords Security Tip (ST04-014) - Avoiding Social Engineering and Phishing Attacks Ransomware Guide (September 2020) Alert AA20-014a - Critical Vulnerabilities in Microsoft Windows Operating Systems Alert AA20-120a - Microsoft Office 365 Security Recommendations Alert AA20-006A - Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad Security Tip (ST18-001) - Securing Network Infrastructure Devices
Center for Internet Security (CIS)	Intel Insights: How to Disable Remote Desktop Protocol CIS Security Controls EI-ISAC Cybersecurity Spotlight – Principle of Least Privilege Cybersecurity Spotlight – Defense in Depth (DiD)
National Security Agency	Mitigating Recent VPN Vulnerabilities Top Ten Cybersecurity Mitigation Strategies Segment Networks and Deploy Application-Aware Defenses Detecting Abuse of Authentication Mechanisms
Federal Trade Commission	Cybersecurity for Small Business