



Authentication controls

Are you effectively using authentication controls to help protect public monies?

Effectively Using Authentication Controls




Why are we issuing this alert?

In August 2024, we issued a financial investigation report revealing an alleged \$39,472,100 loss of public monies over a 10-year period that involved improper use of authentication controls.¹ Specifically, our findings indicated a former county treasurer bypassed these controls and made unauthorized wire transfers from county treasurer accounts to business bank accounts connected to her. The treasurer was able to make these unauthorized wire transfers by herself without detection after she and the chief deputy treasurer shared their passwords and kept their multifactor token authentication devices accessible to one another. This alert outlines what different authentication controls are, why they are important to the integrity of your system, and what actions you can take to ensure they are effectively used to help protect the public monies you manage.

What are authentication controls?

Authentication controls are factors that verify a user's identity for allowing access to protected digital and physical systems and the data they contain. Common authentication factors include passwords, tokens, and biometrics. As illustrated below, these factors can be grouped into 3

Credential categories for common authentication factors:

Something you know	Something you have	Something you are
		
<ul style="list-style-type: none">▶ Password▶ PIN	<ul style="list-style-type: none">▶ Security token device▶ Verification text/email	<ul style="list-style-type: none">▶ Facial recognition▶ Fingerprint

¹ See Arizona Auditor General, *Former Santa Cruz County Treasurer—Alleged Financial Misconduct*, Report 24-402.

Factors from 2 or more of the credential categories described previously can be used together to effect a multifactor authentication (MFA) process, thereby helping to further strengthen security.¹ If used properly, MFA can help protect public monies from both external and internal threats.

External threats include attackers who have gained a compromised password and may break into a protected system if an additional MFA security layer such as a token device or fingerprint is not required for access. Internal threats include employees who fail to properly use MFA by sharing and/or not safeguarding their credentials such as passwords and token devices. Such failure to properly utilize MFA processes can result in unauthorized transfers of public monies.

What actions can you take to ensure authentication controls are effectively used and thereby help you protect public monies?

- 1.** Provide ongoing training to all employees to emphasize the importance of strong internal controls and how properly using and safeguarding authentication factors enforces those controls.
- 2.** Implement MFA for protected digital and physical systems and the data they contain.
- 3.** Establish and enforce a written information technology access and authentication policy that:
 - ▶ Prohibits sharing passwords and other authentication devices.
 - ▶ Prohibits writing down passwords or sending them via an unencrypted mechanism.
 - ▶ Clearly identifies appropriate practices for protecting passwords and safeguarding authentication devices.
 - ▶ Requires immediate reporting of lost, stolen, or compromised authentication devices.
 - ▶ Describes a process for employees to report suspected security incidents related to improper use of passwords and authentication devices.
 - ▶ Defines possible disciplinary actions, up to and including termination, for violations of the policy.
- 4.** Implement an organization-wide password-management system that allows the organization to administer accounts and employees to securely store credentials.
- 5.** Ensure employees document their understanding of the information technology access and authentication policy in writing.
- 6.** In main work areas, post visible reminders of key information technology access and authentication policy elements.
- 7.** Conduct periodic unannounced reviews of internal control procedures to ensure employees are properly using and safeguarding passwords and authentication devices.

¹ Multifactor authentication is also called strong authentication or two-factor authentication.