ZENPRIVATA®

CDFI SECURITY AND PRIVACY FRAMEWORK

Sponsored by:

African American Alliance of CDFI CEOs

Table Of Contents

Introduction & Methodology

ZenPrivata was commissioned by the African American Alliance of CDFI CEOs to develop a security and privacy framework for Community Development Financial Institutions (CDFI) as part of their Women-Led Initiative Technology Enhancement Project (WLITEP).

The CDFI Security and Privacy Framework (CDFI-SPF) was created specifically with the needs and abilities of CDFIs in mind. We met with CDFIs and learned what dangers they face, what risks would be most harmful to CDFIs, what systems CDFIs use and what their attack surface looked like, and what controls CDFIs typically already had in place.

We found that most CDFIs face two concerns:

- The first is that CDFIs hold a lot of sensitive personal information and that their reputation would be damaged if that sensitive information were exfiltrated. Some CDFIs also were subject to privacy regulations through government programs like the US Department of Housing and Urban Development.

- The second is that CDFIs face a surprising number of attempts from attackers to imitate an executive, prompting a financial officer to send CDFI funds to the attacker's bank account.

For the CDFI-SPF, we selected security and privacy controls that will have the most impact on these two concerns, along with other best-practices.

CDFIs also often have limited resources. For this reason, we also tried to choose security and privacy controls that are simpler to implement and provide the most impact for the smallest cost.

This document is designed to be an active document. It begins with a summary of the controls included in the CDFI-SPF and a checklist that CDFIs can use to track their progress in implementing the CDFI-SPF. After that, CDFIs can find more detailed explanations for each control and a set of steps required to implement the control.

The CDFI-SPF was designed to be simpler than many security frameworks. However, the CDFI-SPF includes many controls that require management by the CDFI and requires a significant effort that can quickly become complicated and difficult to manage. For this reason, we recommend that CDFIs manage their implementation of the CDFI-SPF in a compliance platform.

CDFIs can manage the CDFI-SPF in the ZenPrivata platform, which can be found at ZenPrivata.com. Here, CDFIs can manage their progress against the framework and work on the CDFI-SPF controls in a collaborative manner with their teams and any outsourced IT partners or managed service providers.

Access to the ZenPrivata platform is provided free of charge to the CDFIs taking part in the Women-Led Initiative Technology Enhancement Project, thanks to the contribution by the African American Alliance of CDFI CEOs. For CDFIs that are not part of this program, ZenPrivata offers discounted access to its platform to CDFIs, upon request.

CDFI FRAMEWORK CHECKLISTS

ZENPRIVATA®

Contact Us
hello@zenprivata.com
ZenPrivata.com

1. Planning & Assessing

1.1 Risk Assessment

□ Identify Relevant Risks
□ Analyze the Likelihood of Each Risk
□ Analyze the Impact of Each Risk
□ Rank the Risks
□ Maintain a Risk Register
□ Integrate Risk Assessment into Decision-Making

1.2 Data Mapping

□ Identify Data Sources
□ Determine Data Storage Locations
□ Identify Third-Party Data Sharing
□ Build Data Map
□ Integrate Risk Assessment into Decision-Making

1.3 System Inventory

□ Identify Assets
□ Prioritize Assets
□ Integrate with Risk Assessment & Decision-Making

2. Protecting Sensitive Data

2.1 Data Loss Prevention

□ Identify Sensitive Data to Protect
□ Deploy DLP Technology
□ Conduct Regular Testing and Audits

2.2 Breach Detection

□ External, Internal, or Both?
□ Configure External Monitoring Tool
□ Install and Configure an Intrusion Detection System
□ Monitor Regularly

2.3 Breach Response

□ Develop a Breach Response Plan
□ Establish Communication Protocols
□ Conduct Yearly Tabletop Simulations
□ Hold Lessons Learned Sessions
□ Review and Update the Plan

3. Privacy

3.1 Privacy Rights

□ Determine Which Privacy Rights to Provide
□ Data Subject Access Request (DSAR) Process
□ Designate a Privacy Team or Responsible Person
□ Verify Identity
□ Establish a Timeline for Responses

3.2 Privacy Notice

□ Draft Privacy Notice
□ Publish Privacy Notice
□ Regularly Review and Update the Notice

3.3 Privacy Impact Assessment

□ Conduct a Privacy Impact Assessment
□ Document the PIA
□ Review and Approve the PIA

4.1 Stopping Bad Attachments

4.1 Anti-Phishing Controls

□ Enable Anti-Phishing Features in Email Systems
□ Implement Email Filtering Solutions
□ Conduct Phishing Simulations

4.2 Stopping Bad Attachments

□ Implement Email Attachment Scanning Solutions

4.3 Secure File Sharing

□ Choose a Secure File Sharing Solution
□ Implement Access Controls
□ Educate Employees on Secure Sharing Practices

4.4 SPF, DKIM, and DMARC

□ Set Up SPF
□ Set Up DKIM
□ Implement DMARC
□ Test the Configuration

5. Technical Controls for Users

5.1 Multi-Factor Authentication

□ Enforce MFA on All Systems
□ Integrate MFA with IAM System
□ Monitor and Enforce MFA Usage

5.2 Malware Detection

□ Choose the Right Endpoint Protection Software
□ Implement Real-Time Malware Detection
□ Perform Regular Malware Scans
□ Ensure Automatic Updates for Endpoint Protection Software

5.3 Idle Session Timeout

□ Determine Timeout Duration
□ Apply Timeout Settings Across All Systems
□ Communicate Policies to Users

5.4 Full Disk Encryption

□ Choose an Encryption Solution
□ Enable Encryption on Devices
□ Verify Encryption Status
□ Test Recovery Processes

6. Technical Controls for the Organization

6.1 Backups

□ Determine Backup Requirements
□ Determine Continuity and Recovery Objectives
□ Select Backup Solution
□ Implement Backup Schedules
□ Test Backups Regularly

6.2 Automated Patching

□ Assess Patch Management Requirements
□ Select an Automated Patching Solution
□ Establish Patch Deployment Schedules
□ Test Patches Before Deployment

6.3 Vulnerability Scanning

□ Choose a Scanning Tool
Perform Regular Scans
□ Prioritize Results
□ Patch and Mitigate
□ Document and Track Progress

6.4 Audit Logging

□ Define Audit Logging Requirements
□ Select Logging Tools
□ Enable Regular Log Reviews
□ Conduct Log Retention and Archiving

7. The Human Element

7.1 Security & Privacy Training

□ Identify Training Needs
□ Determine a Training Cadence
□ Select Learning Management System
□ Incorporate Simulated Attacks and Exercises
□ Track Attendance and Completion

7.2 Password Management

□ Choose a Password Manager
□ Train Employees
□ Mandate Password Manager Use

7.3 Background Screening

□ Define the Scope of Screening
□ Select a Screening Provider
□ Conduct Role-Specific Checks
□ Integrate Background Screening into Onboarding
□ Establish Clear Criteria for Decision-Making
□ Train Hiring Teams

8. Administrative Controls

8.1 Financial Transaction Procedures

□ Define Approval Hierarchies and Thresholds
□ Separate Financial Accounts
□ Use a Standardized Intake Form for All Requests
□ Require Multiple Approvals for Outgoing Funds
□ Conduct Regular Audits and Reviews

8.2 Vendor Management

□ Identify and Categorize Vendors
□ Conduct Vendor Risk Assessments
□ Integrate Security and Privacy Requirements into Contracts
□ Maintain a Vendor Risk Register
□ Integrate Risk Assessment into Decision-Making

8.3 Account Granting & Revocation

□ Create Account Change Request Process
□ Establish Timely Account Revocation Procedures
□ Implement Idle Account Monitoring and Cleanup
□ Maintain detailed records

1. Planning & Assessing

Organizations are unique, shaped by their missions, operations, and the communities they serve, and CDFIs are no exception. CDFIs face a distinct set of risks. And, if those risks were to come true, the impact of those risks would be different for CDFIs than for other types of organizations. Adding to this complexity, no two CDFIs share the same risk profile. Factors such as size, location, client base, and technological infrastructure can significantly influence the nature and severity of the risks they face.

For this reason, the CDFI-SPF begins with planning and assessing. Strong security and privacy programs begin with a thorough understanding of their organization’s unique needs, potential risks, and strategic priorities. This involves scrutinizing existing processes, technologies, and data handling practices to uncover gaps, vulnerabilities, and areas for improvement. By dedicating time and resources to this critical first step, CDFIs can build a resilient and secure environment that supports their mission.

This proactive approach allows CDFIs to focus their efforts on areas that will have the greatest impact, ensuring that security investments are efficient and effective. The insights gained from planning and assessing can guide CDFIs toward more meaningful, impactful improvements. Ultimately, this foundational work strengthens CDFIs’ ability to anticipate challenges, adapt to evolving threats, and create a resilient, secure environment that supports long-term goals.

1. Planning & Assessing Controls:

1.1 Risk Assessment

1.2 Data Mapping

1.3 System Inventory

1.1 Risk Assessment

Risk assessment is a foundational practice for identifying, analyzing, and addressing potential threats to a CDFI’s operations, data, and systems. By systematically evaluating risks, CDFIs can determine the likelihood and impact of potential incidents and prioritize actions to mitigate those risks. This proactive approach helps optimize the allocation of resources.

A thorough risk assessment involves examining both external threats, such as cyberattacks or regulatory changes, and internal risks, such as outdated processes, insider threats, or human error. The process typically includes identifying critical assets, evaluating existing controls, and mapping out potential scenarios that could disrupt operations. Based on these findings, CDFIs can implement targeted strategies to reduce risk.

Conducting regular risk assessments also enables CDFIs to stay agile in the face of evolving threats. As technologies, business needs, and regulatory environments change, reassessing risks ensures that security and privacy programs remain effective and aligned with current challenges.

What to do:

- ***Identify Relevant Risks:*** This should include both internal and external risks.
- ***Analyze the Likelihood of Each Risk:*** This is an estimation of how probable it is that the risk occurs. This can be a number, a percentage, or high/medium/low.
- ***Analyze the Impact of Each Risk:*** This is a determination of, if we assume the risk has occurred, what is the impact? This can be a number, a dollar amount, or high/medium/low.
- ***Rank the Risks:*** Combine the likelihood and impact of each risk into a total risk level. Then, rank the risks in order of highest to lowest.
- **Maintain a Risk Register:** Record all identified risks and risk levels in a centralized risk register.
- ***Integrate Risk Assessment into Decision-Making:*** Use the results to inform strategic decisions, such as investments in security technologies, updates to policies, or resource allocation.

1.2 Data Mapping

Data mapping is the process of identifying, categorizing, and organizing where sensitive data is stored, processed, and transmitted across a CDFI's systems. It provides a comprehensive view of the flow of information, highlighting where data originates, where it moves, and where it is ultimately stored or archived.

Through data mapping, a CDFI can identify areas where sensitive information, such as personally identifiable information (PII) or financial data, is collected, processed, and transmitted. This insight enables a CDFI to understand not only what data the CDFI holds but also how it is being accessed and used, ensuring that it is only processed by authorized individuals and systems.

A well-executed data map helps identify potential vulnerabilities in data storage or processing and can guide improvements in security measures to protect sensitive information. Ultimately, data mapping is not only an essential part of data governance but also a proactive strategy to ensure a CDFI is handling personal and sensitive information in a secure, responsible, and compliant manner.

What to do:

- ***Identify Data Sources:*** List all the sources where data is collected, such as customer forms, online transactions, third-party vendors, or internal systems. This can include both digital and physical sources.
- ***Determine Data Types:*** For each data source, determine which categories of data are collected. Note where the most sensitive data is stored.
- ***Determine Data Storage Locations:*** Identify where each type of sensitive data is stored, both on-premises and in the cloud. This might include places like databases, servers, file systems, backups, and physical storage locations like filing cabinets.
- ***Identify Third-Party Data Sharing:*** Identify any external parties that receive or process your data (e.g., vendors, contractors, service providers) and document any data sharing agreements.
- ***Build Data Map:*** Record the information into a spreadsheet and a visual diagram showing the flow of data in your organization.
- ***Integrate Risk Assessment into Decision-Making:*** Use the results to inform strategic decisions regarding data collection, retention and protection.

1.3 System Inventory

A system inventory is a comprehensive and organized record of all the technology, hardware, software, networks, and digital tools used within a CDFI. This includes everything from computers, servers, and mobile devices to applications, operating systems, and network infrastructure. By documenting all technological assets in one centralized list, CDFIs can gain a clear understanding of their technology landscape, ensuring they know exactly what resources are available and how they are being used.

The importance of maintaining a system inventory lies in its ability to provide visibility into the CDFI's tech ecosystem. It helps ensure that all systems and devices are properly accounted for and can be used to ensure that any outdated, unused, or unsupported technology is identified and addressed.

A well-maintained system inventory can streamline operational efficiency by preventing redundant technology purchases, simplifying troubleshooting, and aiding in system upgrades or replacements. A system inventory is an essential tool for maintaining control over a CDFI’s technology infrastructure.

What to do:

- ***Identify Assets:*** Identify all systems, applications, and services. Note which are third-party systems.
- ***Prioritize Assets:*** Prioritize these systems in order of importance.
- ***Integrate with Risk Assessment & Decision-Making:*** Use the inventory to inform risk management strategies, such as prioritizing systems for security upgrades or replacements, and integrate the inventory into organizational decision-making regarding resource allocation, security investments, and compliance planning.

2. Protecting Sensitive Data

CDFIs handle substantial amounts of sensitive data, ranging from personal and financial information of customers to proprietary business details. This data is not only critical for daily operations but also forms the backbone of trust between CDFIs and their customers. Protecting sensitive information is paramount to ensuring the success, integrity, and long-term viability of CDFIs.

Sensitive data, such as customer profiles, loan applications, financial records, and operational details, is one of a CDFI's most valuable assets. Mishandling or exposing this data can lead to significant consequences, including financial loss, legal liabilities, regulatory penalties, and reputational damage.

For this reason, data protection is critical to the success and integrity of CDFIs. By implementing strong data protection practices, such as encryption, secure access controls, and regular risk assessments, CDFIs can reduce the risk of data breaches and unauthorized access. These measures not only help comply with any legal and regulatory requirements but also enhance operational resilience and minimize disruptions caused by potential security incidents.

Protecting sensitive data builds and sustains customer trust—a vital component for the success of CDFIs. Customers and stakeholders are more likely to engage with and support institutions they perceive as reliable and secure. Demonstrating a commitment to privacy and security strengthens a CDFI's reputation, reinforces client relationships, and positions the organization as a dependable partner in the financial ecosystem.

2. Protecting Sensitive Data Controls:

2.1 Data Loss Prevention

2.2 Breach Detection

2.3 Breach Response

2.1 Data Loss Prevention

Data Loss Prevention (DLP) tools help protect sensitive information by preventing it from being accidentally shared or intentionally leaked outside your organization. DLP software actively monitors and controls how data is accessed, used, and transmitted. By applying predefined rules and policies, DLP tools can identify, classify, and track sensitive information like personally information, financial records, intellectual property, and confidential business data.

The primary function of DLP tools is to block risky actions that could lead to the exposure of sensitive data, such as sending confidential files through unsecured or unauthorized channels like personal email accounts, file-sharing platforms, or external devices. These tools typically scan for data patterns (e.g., credit card numbers, Social Security numbers) and use contextual analysis to ensure that data is only shared or transmitted through approved and secure methods.

By implementing DLP on your organization's most sensitive data, you reduce the risk of data breaches, which could otherwise result in significant financial losses, reputational damage, or regulatory penalties. DLP tools not only help prevent external threats but also mitigate internal risks, such as employees accidentally sending sensitive information to the wrong recipients or malicious insiders attempting to leak data. This makes DLP a critical component of an organization's overall data protection strategy.

DLP tools are a vital layer of defense for any organization looking to protect its data, uphold privacy standards, and preserve its reputation.

What to do:

- ***Identify Sensitive Data to Protect:*** Based on your risk assessment and data map, determine what type of information you want to subject to DLP, such as personal information or financial records.
- ***Deploy DLP Technology:*** Select and deploy a DLP solution to monitor, detect, and prevent unauthorized access, sharing, or exfiltration of the types of sensitive data selected in step 1.
- ***Conduct Regular Testing and Audits:*** Test DLP systems regularly to identify gaps, false positives, or areas where policies need adjustment

2.2 Breach Detection

Breach detection is the process of identifying unauthorized access to or compromise of an organization's systems, networks, or data. It focuses on detecting security incidents quickly so that organizations can respond promptly to mitigate damage, protect sensitive information, and prevent further exploitation. Breach detection solutions use a combination of monitoring, analytics, and threat intelligence to identify suspicious activities or anomalies that may indicate a breach..

The first, external monitoring, involves actively monitoring the internet and dark web for indicators of a security breach, such as leaked accounts, compromised credentials, or stolen sensitive data being shared or sold. This approach leverages threat intelligence tools and services that continuously scan public forums, social media platforms, paste sites, and dark web marketplaces for evidence of data exposure. These tools can flag suspicious activity, such as credentials matching your organization's domain, allowing you to respond quickly and take remedial action, like resetting passwords or securing affected systems.

The second, **internal monitoring**, is done by using breach detection tools to monitor network traffic, analyze system logs, and deploy intrusion detection systems (IDS) to spot potential indicators of compromise. Advanced systems may incorporate machine learning and artificial intelligence to detect subtle patterns or behaviors that human analysts might miss, such as unusual login attempts, unauthorized data transfers, or unexpected changes in system configurations. These tools can also correlate events across multiple systems to uncover sophisticated attacks that evade traditional defenses. IDS tools, however, can be expensive for CDFIs.

The importance of breach detection lies in its ability to minimize the impact of a security incident. By identifying a breach quickly, organizations can take immediate action to contain the threat, secure affected systems, and prevent data loss. This rapid response is critical for protecting sensitive information, maintaining business continuity, and preserving customer trust. In today's rapidly evolving threat landscape, breach detection is a cornerstone of a proactive cybersecurity strategy.

What to do:

- ***External, Internal, or Both?:*** Decide, based on your CDFI's budget and risks, whether your organization should employ external monitoring, internal monitoring, or both.
- ***Configure External Monitoring Tool:*** Deploy an external monitoring tool to scan the internet and dark web for leaked credentials, sensitive information, or indicators of a breach. Use the insights from these tools to take proactive action, such as resetting compromised credentials or strengthening security measures.
- ***Install and Configure an Intrusion Detection System (if applicable):*** Choose an IDS that fits your organization's needs, such as a host-based or network-based system. Ensure the IDS is configured to notify your team immediately when suspicious activity is detected.
- ***Monitor Regularly:*** Regularly review alerts to identify trends or attempts that could indicate ongoing threats. Use the insights from these tools to take proactive action, such as resetting compromised credentials or strengthening security measures.

2.3 Breach Response

Breach response is a critical component of any security strategy, ensuring that your organization is prepared to quickly and effectively handle security incidents. When a breach occurs, it is essential to have a well-defined plan in place to minimize damage, contain the threat, and recover swiftly. A strong breach response plan includes clear steps for identifying the breach, notifying affected stakeholders, and investigating the cause of the incident.

Having a well-coordinated response can limit the impact on your systems, data, and reputation. It also ensures compliance with legal and regulatory requirements, such as breach notification laws, which help you avoid penalties and legal liabilities.

A proactive breach response plan also involves regular testing and updates to ensure that your team is ready to act at a moment's notice. By being prepared, you not only reduce the risk of significant damage but also demonstrate your commitment to safeguarding your organization and the trust of your clients and partners.

What to do:

- ***Develop a Breach Response Plan:*** Create a detailed, actionable plan outlining steps to take in the event of a breach, including identification, containment, and recovery processes. Ensure all team members know their roles and responsibilities.
- ***Establish Communication Protocols:*** Create a clear communication strategy to notify all relevant stakeholders (employees, customers, regulators) in the event of a breach. Ensure timely and transparent updates are provided.
- ***Conduct Yearly Tabletop Simulations:*** Regularly run breach response simulations with key team members to test the plan and improve coordination. These exercises allow your team to practice their response in a controlled environment and identify potential gaps in the process.
- ***Hold Lessons Learned Sessions:*** After a breach or simulation, gather your team to discuss what went well, what could be improved, and any missed opportunities for faster or more effective responses. Use this feedback to refine the plan.
- ***Review and Update the Plan:*** Update your breach response plan based on the simulations and lessons learned sessions and when new threats arise and business needs change.

3. Privacy

Privacy controls are indispensable for CDFIs because they hold individuals' personal data, complementing the data protection controls from the previous section. Beyond protecting the personal data you've collected, it's also important to minimize the collection of personal data and to ensure you're only collecting as little personal information as required to accomplish the business goal.

Privacy controls like these are essential for responsibly collecting personal information and, for some CDFIs, ensuring compliance with privacy laws and regulations. By implementing robust privacy controls, CDFIs can further build trust with clients, employees, and stakeholders. These measures reduce the risk of misuse or exposure of sensitive data and demonstrate a CDFI's commitment to protecting the privacy of their customers and partners.

Privacy controls are indispensable for CDFIs because they hold individuals' personal data. Effective privacy controls foster a culture of transparency and accountability within an organization. These measures reduce the risk of misuse or exposure of sensitive data, while demonstrating a CDFI's commitment to safeguarding the privacy of their customers and partners.

3. Privacy Controls:

3.1 Privacy Rights

3.2 Privacy Notice

3.3 Privacy Impact Assessment

3.1 Privacy Rights

Customers should feel confident that they can easily access, manage, and control their personal data. CDFIs can foster this confidence by providing clear and easy ways for customers to exercise their privacy rights. These rights typically include the ability to access their personal data, update it if it's incorrect, delete it when it's no longer necessary, and opt out of specific types of data processing, such as marketing communications or sharing data with third parties.

By offering these privacy rights, CDFIs demonstrate a commitment to transparency and customer empowerment, allowing individuals to feel in control of their own information. The ability to access personal data lets customers see exactly what information the institution holds about them, giving them a better understanding of how their data is used. Allowing customers to update or correct their data ensures that the information is accurate and up to date, which is especially important for organizations that rely on accurate data for decision-making or service delivery.

Offering the right to delete data also helps ensure that individuals' personal information is only retained for as long as it's necessary for business purposes. Customers may feel more secure knowing that they can request the removal of outdated or irrelevant data, giving them a sense of control over their digital footprint. Additionally, enabling customers to opt out of certain types of data processing, such as marketing activities or the sharing of data with third parties, reinforces the idea that they have control over how their data is used and distributed.

When CDFIs offer these rights, they help build customer trust by showing that they value and protect the personal information their customers provide. Customers who feel their data is handled responsibly are more likely to develop long-term loyalty to an organization. This sense of trust is critical in an age where data breaches and privacy concerns are increasingly prevalent, and individuals are more aware of their rights regarding personal data.

What to do:

- ***Determine Which Privacy Rights to Provide:*** Customers have a range of privacy rights that CDFIs can provide, such as the right to request information about the personal data an organization holds about them, the right to correct inaccurate or incomplete personal data, the right to request the deletion of personal data, the right to object to the processing, the right to obtain a copy of personal data in a structured, portable format, the right to object to processing, and the right to withdraw consent.
- ***Data Subject Access Request (DSAR) Process:*** Give individuals a place to make requests to exercise their privacy rights (typically on your website or by e-mail) and set up a system to track and manage customer requests.
- ***Designate a Privacy Team or Responsible Person:*** Designating a dedicated team or individual to oversee privacy rights requests ensures that the process is managed efficiently and consistently.
- ***Verify Identity:*** To prevent unauthorized access to personal data, CDFIs should implement procedures for verifying the identity of individuals making privacy requests.
- ***Establish a Timeline for Responses:*** Determine the time frame in which to respond to privacy requests, such as within 30 days or 45 days.

3.2 Privacy Notice

To achieve transparency, CDFIs should clearly communicate the types of information they collect, such as names, contact details, browsing behaviors, or payment information, and explicitly state the purposes for which this data is used—whether for processing transactions, personalizing experiences, or improving services. Transparency also involves disclosing where data processing will take place, whether locally, remotely, or across international borders, and specifying how long the data will be retained. CDFIs should also indicate if the data will be shared with third parties, such as service providers or marketing partners, and provide details about the nature of such transfers.

This communication is often delivered through a privacy notice, typically accessible on a website. A well-crafted privacy notice serves as the foundation for transparency. It should be written in plain language that is easy for the average person to understand, avoiding overly technical jargon or complex legal terminology. Essential details, such as the CDFI's identity, contact information, and a summary of individuals' rights concerning their data, should be prominently displayed.

Hiding critical information within dense blocks of legal text or obscure sections of a website not only undermines transparency but can also breach legal and ethical standards.
Ultimately, transparency is about respecting individuals' autonomy and rights over their personal information. By being clear and open about data practices, CDFIs can build lasting relationships with customers, enhance their reputation, and demonstrate a commitment to responsible data stewardship.

What to do:

- ***Draft Privacy Notice:*** Be sure to include things like what your organization collects, for what purposes, whether that data is shared, retention periods, security measures, cookie usage and tracking, a contact point, and which privacy rights are available to users, as your organization determined in control 3.1.
- ***Publish Privacy Notice:*** Typically this will be on the organization website.
- ***Regularly Review and Update the Notice:*** Establish a process to periodically review and update the privacy notice to reflect changes in laws, business practices, or data processing activities. Include a "last updated" date on the privacy notice for transparency.

3.3 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a process that helps organizations identify and minimize the risks associated with the processing of personal data. It is designed to evaluate the impact of data processing activities on the privacy and security of individuals, ensuring that potential risks are understood and mitigated before any processing begins. For organizations like CDFIs, conducting a PIA is a proactive step in demonstrating their commitment to safeguarding customer data and protecting individuals' privacy.

The PIA process involves assessing the type of data being collected, how it will be used, who will have access to it, and the potential risks to individuals' privacy rights. It helps organizations evaluate whether the data processing activities are necessary, whether there are less invasive alternatives, and whether appropriate security measures are in place to protect the data. By conducting a PIA, CDFIs can identify and address risks early on, which helps prevent data breaches, unauthorized access, or misuse of personal information.

In the context of CDFIs, performing a PIA is particularly important when implementing new projects or systems that involve sensitive customer data. For example, if a CDFI plans to launch a new digital platform or introduce a new service that involves processing personal data, a PIA ensures that the privacy implications are carefully considered. The assessment evaluates not only the technical and organizational safeguards in place but also how transparent and accountable the organization is in its data processing activities.

Once the PIA is completed, organizations should implement measures to mitigate identified risks, such as enhancing security protocols, minimizing data collection, or providing customers with more control over their data. Regular reviews of the PIA process are also important to ensure that it remains effective and up to date as new risks emerge or changes occur in data processing practices.

By conducting a PIA, CDFIs not only demonstrate a commitment to responsible data practices but also help protect their customers from potential privacy harms. It is an essential tool for building trust and ensuring that customer data is handled in a way that respects individual rights and complies with best practices in privacy.

What to do:

- ***Conduct a Privacy Impact Assessment***: Determine if the processing of personal data is likely to result in risks to individuals, describe the data collection and processing, assess the necessity and whether the data collection is proportional to the goal, and implement safeguards against the risks.
- ***Document the PIA***: Maintain detailed documentation of the PIA process, including the assessment of risks, mitigation strategies, and consultations with stakeholders. Ensure that the final PIA report is accessible for review.
- ***Review and Approve the PIA***: Ensure that the PIA is reviewed by the appropriate internal team (e.g., privacy, legal, risk management) and approved before the processing begins. Document the approval process and keep a record of any concerns raised during the review.

4. Securing E-Mail

CDFIs are increasingly becoming targets for cybercriminals, particularly through phishing attacks, due to the nature of their financial operations and the sensitive data they handle. Cybercriminals often exploit the nature of financial operations, which involve regular communication with clients, partners, and employees, to launch highly targeted attacks. In a phishing scheme targeting CDFIs, attackers may impersonate trusted partners, clients, or even internal colleagues, leveraging social engineering tactics to manipulate individuals into clicking on malicious links, opening dangerous attachments, or providing sensitive information. Once the attacker has gained access to systems or accounts, they can divert funds to their own accounts or steal confidential data, wreaking havoc on the organization’s operations and reputation.

The consequences of a successful email attack are severe. Not only can such attacks compromise financial transactions and result in direct financial loss, but they can also expose sensitive customer information, internal communications, and proprietary data. This breach of confidentiality could damage the trust customers have in the organization, leading to long-term reputational harm, regulatory scrutiny, and potential legal consequences.

For this reason, email security is absolutely crucial. A well-implemented email security system acts as the first line of defense against phishing and other email-based attacks. Ultimately, by committing to strong email security practices, CDFIs can build a resilient defense against cybercriminals. This not only protects financial assets but also reinforces the organization's dedication to safeguarding customer data, ensuring business continuity, and maintaining the trust of clients, partners, and the broader community.

4. Securing E-Mail Controls:

4.1 Anti-Phishing Controls

4.2 Stopping Bad Attachments

4.3 Secure File Sharing

4.4 SPF, DKIM, and DMARC

4.1 Anti-Phishing Controls

Anti-phishing controls are crucial for protecting both individuals and organizations from phishing attacks, which are a common method cybercriminals use to gain access to sensitive information, steal credentials, or distribute malware. Phishing attacks often come in the form of deceptive emails, messages, or websites that impersonate trusted entities, such as banks, colleagues, or vendors, in an effort to trick individuals into disclosing personal or confidential information.

One of the primary reasons anti-phishing controls are essential is that they help detect, mark, and sometimes block these deceptive communications before they reach users. Many phishing attacks rely on human error—such as clicking on a malicious link or downloading an infected attachment—to succeed. Anti-phishing controls, such as email filtering controls, can automatically identify and block phishing emails by scanning for known signs of phishing, such as suspicious subject lines, deceptive sender addresses, or embedded links that lead to fraudulent websites.

In addition to protecting against individual attacks, anti-phishing controls help to safeguard an organization's overall security posture. A successful phishing attack can result in unauthorized access to internal systems, financial loss, data breaches, or the spread of malware across the network. Anti-phishing tools, therefore, play a vital role in preventing these threats, ensuring that an organization's systems, networks, and sensitive data remain secure.

Anti-phishing controls are essential for detecting, preventing, and mitigating the impact of phishing attacks. By employing them, CDFIs can reduce the risk of falling victim to phishing schemes and protect their sensitive information from cybercriminals.

What to do:

- ***Enable Anti-Phishing Features in Email Systems:*** Activate built-in anti-phishing tools in your email system, such as warning when an e-mail comes from outside of the organization.
- ***Implement Email Filtering Solutions:*** Deploy email filtering tools that detect and block phishing emails by scanning subject lines, content, and attachments.
- ***Conduct Phishing Simulations:*** Regularly perform simulated phishing attacks to test the effectiveness of your anti-phishing training and controls. Use the results of these simulations to identify weaknesses and provide targeted follow-up training to those who failed the tests.

4.2 Stopping Bad Attachments

Ensuring that bad attachments are identified and blocked is a critical aspect of protecting your organization from malware, ransomware, and other security threats that can be hidden in email attachments. Cybercriminals often use email attachments as a delivery method for malicious software, which can infect your systems, steal sensitive data, or even lock files for ransom. Because email is such a common method of communication, malicious actors frequently exploit it to distribute threats that can bypass traditional security measures.

The first line of defense against these risks is the implementation of robust attachment scanning. Modern email security tools can automatically scan attachments for viruses, malware, and other suspicious content. However, they need to be turned on and configured. By using these detection methods, your organization can prevent harmful files from entering your network.

Many email systems allow for the use of file type restrictions, which can prevent certain types of files —such as executable files or macros—from being sent or received through email. By enforcing these restrictions, organizations can limit the types of attachments that are allowed to pass through, significantly reducing the risk of malicious files slipping through the cracks.

By catching harmful attachments early in the process, organizations can significantly reduce the risk of accidental downloads and prevent malware, ransomware, or other harmful software from infiltrating their systems. This proactive approach not only helps protect your network and data but also ensures business continuity by avoiding the disruption caused by security breaches, data loss, or compromised systems. A comprehensive attachment scanning strategy is therefore essential for maintaining a secure email environment and safeguarding the integrity of your organization’s operations.

What to do:

- ***Implement Email Attachment Scanning Solutions:*** Deploy email security solutions that automatically scan email attachments for malicious content, including viruses, malware, ransomware, and phishing exploits.

4.3 Secure File Sharing

Secure file sharing is crucial for protecting sensitive information while maintaining efficient collaboration across your organization. Sharing files through a secure file system is generally much safer than using email for several key reasons. First, email is inherently less secure, as it often lacks built-in encryption, making it vulnerable to interception. Even if an email is sent securely, the files attached to it may not be protected, leaving them exposed during transit. In contrast, secure file systems typically use encryption both in transit and at rest, ensuring that files are protected throughout the entire sharing process, from upload to download.

Another advantage of secure file systems is their ability to offer granular access controls. While email allows files to be forwarded easily and without restrictions, secure file systems let you set permissions on who can view, edit, or share a file. This minimizes the risk of unauthorized access or accidental exposure, which is common when files are shared via email. With a secure file system, you can limit access to only those individuals who need it, and track who has accessed or modified the file.

Secure file systems also provide centralized storage, making it easier to manage and organize files. Unlike email, where files are scattered across multiple inboxes and folders, secure file systems allow for easy tracking, searching, and retrieval of documents, reducing the chances of misplacing or losing critical information. Additionally, version control features in secure file systems enable you to maintain a history of file changes, providing a clear record of edits and updates, which is not possible with email attachments.

Email systems are also more prone to phishing attacks and malware, which can be easily embedded in attachments or links. Even with email security tools in place, malicious actors often exploit human error, such as clicking on a seemingly legitimate attachment. Secure file systems, on the other hand, are typically designed to mitigate these risks by offering secure authentication methods, encryption, and real-time monitoring of file-sharing activities.
Lastly, secure file systems provide an audit trail that records who accessed or interacted with files, creating a record of activity that can be reviewed if needed. This is crucial for organizations that need to comply with data protection regulations and maintain a high level of accountability. Email lacks this kind of monitoring, making it difficult to track who has seen or interacted with files, and leaving a gap in auditability.

While email may seem convenient for file sharing, a secure file system provides superior protection, better access management, and stronger tracking capabilities. By using secure file systems, organizations can reduce risks, improve collaboration, and ensure that sensitive data is handled responsibly.

What to do:

- ***Choose a Secure File Sharing Solution:*** Select a platform that offers end-to-end encryption, access controls, and audit logs to ensure the security of files during sharing and storage.
- ***Implement Access Controls:*** Ensure that only authorized individuals can access sensitive files. Enforce the principle of least privilege, giving the minimum level of permissions needed.
- ***Educate Employees on Secure Sharing Practices:*** Train employees on best practices for securely sharing files, including avoiding sharing files via unsecured platforms like email or unsecured cloud storage. Emphasize the importance of using secure links and password-protected files.

4.4 SPF, DKIM, and DMARC

To reduce the likelihood of spoofed or modified emails from legitimate domains, it's essential to implement a DMARC (Domain-based Message Authentication, Reporting, and Conformance) policy along with email verification tools such as Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). These email authentication protocols are critical in defending against email spoofing and phishing attacks, which are common tactics used by cybercriminals to deceive recipients into believing they're receiving messages from trusted sources.

The first step in this process is configuring SPF for the CDFI's domain. SPF is an email authentication standard that allows domain owners to specify which mail servers are permitted to send emails on their behalf. When an email is received, the receiving mail server checks the SPF record of the sending domain to verify whether the email comes from an authorized source. If the email fails this check, it may be marked as suspicious or rejected outright. By implementing SPF, CDFIs can prevent unauthorized senders from using your domain to send fraudulent emails, significantly reducing the risk of spoofing attacks.

Next, DKIM provides an additional layer of security by adding a digital signature to outgoing emails. This signature is created using a private key held by the sender's mail server and is included in the email's header. The receiving mail server can then use the sender's public key, which is published in the DNS records, to verify the authenticity of the signature. If the signature matches, it confirms that the email has not been altered in transit and that it indeed came from the expected sender. DKIM ensures that the integrity of the email is maintained, protecting your organization from the risks of email tampering or modification by malicious actors.

While SPF and DKIM help ensure the authenticity of the sender and the integrity of the message, DMARC ties these two protocols together and provides an additional layer of protection. DMARC allows domain owners to specify how email receivers should handle emails that fail SPF or DKIM checks, whether by rejecting, quarantining, or allowing the email to pass with a warning. DMARC also provides reporting features, allowing organizations to monitor how their domain is being used in email communications and detect any unauthorized use or potential attacks.

Implementing DMARC with SPF and DKIM can significantly reduce the risk of phishing and email spoofing attacks. These attacks often aim to exploit the trust between organizations and their customers, partners, or employees. By ensuring that emails are authenticated and verifying that they come from legitimate sources, CDFI's can protect both the brand's reputation and the security of the individuals who rely on the CDFI's communications. Additionally, these measures help prevent attackers from impersonating the CDFI and using the domain to send fraudulent or malicious messages that could lead to data breaches, financial loss, or other severe consequences.

Implementing DMARC, along with SPF and DKIM, is a proactive strategy that helps secure CDFI email communications by preventing spoofed or modified emails from valid domains. By adopting these tools, a CDFI can protect from phishing, enhance your email security posture, and safeguard your brand's reputation from malicious actors.

What to do:

- ***Set Up SPF (Sender Policy Framework):*** Create an SPF record in your domain's DNS settings that specifies which IP addresses are authorized to send emails on behalf of your domain. Include all mail servers that are used to send emails, including third-party services (e.g., email marketing platforms). Test and validate the SPF record to ensure it is configured correctly and prevents unauthorized senders.
- ***Set Up DKIM (DomainKeys Identified Mail):*** Generate DKIM keys for your domain and configure your mail server to sign outgoing emails with these keys. Publish the public key in your domain's DNS settings so that recipients can verify the authenticity of the email. Test DKIM signatures to ensure they are correctly applied and verified by recipient servers.
- ***Implement DMARC (Domain-based Message Authentication, Reporting & Conformance):*** Create a DMARC record in your DNS settings with the appropriate policy to instruct receiving mail servers on how to handle emails that fail SPF or DKIM checks. Include an email address for DMARC reports so you can monitor unauthorized email activity and adjust policies as needed.
- ***Test the Configuration:*** Use online tools like MXToolbox or DMARC Analyzer to test your SPF, DKIM, and DMARC configurations. Send test emails from your domain to third-party services to ensure that the SPF and DKIM checks are passing and that DMARC policies are being enforced.

5 & 6 Technical Controls

Implementing technical controls is a fundamental element of a comprehensive cybersecurity strategy, providing organizations with the tools and systems necessary to safeguard against an ever-evolving array of threats. These controls serve as essential barriers that protect against unauthorized access, detect potential vulnerabilities, and respond to suspicious activity in real time, ultimately minimizing the impact of cyber incidents. By adopting and maintaining robust technical controls, organizations can stay one step ahead of cybercriminals and mitigate the risks that come with managing sensitive information and systems.

Technical controls come in various forms and are designed to address different aspects of cybersecurity. At their core, these controls are built to ensure that only authorized individuals or systems can access critical infrastructure, applications, and data.

By integrating all of these technical controls into their cybersecurity strategy, CDFIs can create a secure environment that ensures the confidentiality, integrity, and availability of their systems and sensitive data. This proactive defense strategy allows CDFIs to confidently support their mission, providing vital financial services to underserved communities while minimizing the risks posed by cyber threats.

Additionally, leveraging these controls not only protects critical infrastructure but also fosters an organizational culture focused on security. With the right technical measures in place, employees and teams can work efficiently, knowing that their work environment is safeguarded against cybercriminals. This security confidence contributes to an organization’s long-term success, as it reduces the likelihood of costly data breaches, service interruptions, or reputation damage.

Technical controls are the backbone of a resilient cybersecurity posture. By proactively implementing access controls, malware protection, encryption, vulnerability management, and real-time monitoring systems, organizations can reduce their exposure to cyber threats and respond rapidly to any potential incidents. For CDFIs, this approach to cybersecurity not only protects sensitive financial data but also strengthens the institution’s ability to carry out its mission while safeguarding the trust of its clients and stakeholders.

5. Technical Controls for Users:

5.1 Multi-Factor Authentication

5.2 Malware Detection

5.3 Idle Session Timeout

5.4 Full Disk Encryption

6. Technical Controls for the Organization:

6.1 Backups

6.2 Automated Patching

6.3 Vulnerability Scanning

6.4 Audit Logging

5. Technical Controls for Users

5.1 Multi-Factor Authentication

Multi-factor authentication (MFA) is a powerful security tool that adds an extra layer of protection to your accounts, making it more difficult for unauthorized individuals to gain access, even if they have stolen your password. Unlike traditional password-only login systems, which rely solely on something you know, like a password, MFA requires additional authentication factors. This is typically something you have, such as a phone or hardware token, or something you are like a fingerprint or facial recognition.

The additional step in the MFA process significantly reduces the likelihood of a successful cyber attack, particularly in cases where hackers have managed to obtain a password. With MFA, even if a malicious actor acquires a user's password through a data breach, phishing scam, or other methods, they would still need access to the second authentication factor (such as the user's phone) to successfully log in. This makes it much more difficult for hackers to bypass security, as they need to compromise multiple layers of security instead of just one.

MFA can be implemented in a variety of ways. One of the most common forms is time-based one-time passcodes, where a user receives a temporary code sent to their phone or email. This code is typically valid for a short period and changes regularly, ensuring that even if someone intercepts the code, it cannot be reused. Another option is push notifications, where the user simply approves or denies a login attempt from a trusted device. More advanced methods use biometric verification, like fingerprint or facial recognition, which offer a highly secure and convenient way to authenticate users.

For CDFI's, MFA is a critical tool for protecting sensitive data, systems, and accounts. With the increasing frequency of cyber attacks targeting user credentials, organizations must implement MFA to ensure that even if an employee's password is compromised, attackers cannot gain access to critical resources. MFA also mitigates the risk of social engineering attacks, such as phishing, where attackers trick users into revealing their passwords. Since the additional authentication factor is typically independent of the password, it prevents attackers from easily exploiting stolen login credentials.

Moreover, MFA enhances overall security hygiene by making it harder for unauthorized users to penetrate systems. As a result, it lowers the likelihood of security breaches, data theft, or fraud. This is particularly important for organizations handling sensitive information or financial transactions, where a single breach could have devastating consequences. Implementing MFA is a relatively low-cost, high-reward security measure that can prevent a wide range of cyber threats.

What to do:

- ***Enforce MFA on All Systems:*** Require MFA for all users on all systems that require users to log-in, including systems hosted by third-party vendors

- ***Integrate MFA with IAM System:*** Ensure that your Identity and Access Management (IAM) platform, such as Microsoft Entra, supports and is integrated with your chosen MFA solution. Configure your IAM system to enforce MFA for logging into applications or systems, particularly those with access to sensitive data or financial transactions.
- ***Monitor and Enforce MFA Usage:*** Track users and systems to ensure that all users have MFA implemented on all systems.

5.2 Malware Detection

Setting an idle session timeout is a simple yet powerful security measure designed to protect your organization from unauthorized access to sensitive systems and data. An idle session timeout works by automatically logging users out of their accounts or locking their sessions after a specified period of inactivity. This ensures that if a user steps away from their device or forgets to log out, their session cannot be exploited by someone else. Without this safeguard, an unattended session could be a gateway for malicious actors to access sensitive information, manipulate systems, or compromise organizational security.

The risk is particularly significant on shared or public devices, where multiple users may have access. For example, an employee working on a personal laptop at a coffee shop might inadvertently leave a session open, allowing the next person to access their account. Idle session timeouts help mitigate this risk by cutting off access as soon as inactivity is detected, effectively locking out unauthorized users.

Moreover, idle session timeouts encourage a culture of security awareness. Employees and users become more mindful of their digital activities, knowing their access will be automatically revoked after a period of inactivity. This awareness can lead to better habits, such as manually logging out or securing devices when stepping away.

When configuring idle session timeouts, it’s important to strike the right balance between security and user convenience. Setting the timeout period too short could frustrate users, leading to inefficiencies or resistance to the policy. Conversely, setting it too long could leave sessions vulnerable to unauthorized access. Best practices often suggest a timeout period that aligns with the sensitivity of the systems and the typical workflow of users.

Idle session timeouts provide an effective way to enhance a CDFI’s security posture. By automatically ending inactive sessions, the CDFI reduces the risk of unauthorized access, safeguards sensitive data, and ensures that systems remain secure.

What to do:

- ***Determine Timeout Duration:*** Assess the nature of your business processes and determine a suitable idle timeout period (e.g., 5, 10, or 15 minutes of inactivity). Balance security needs with user convenience to avoid overly short timeouts that disrupt productivity. Consider industry standards or regulatory requirements that may mandate specific timeout settings.
- ***Apply Timeout Settings Across All Systems:*** Configure idle session timeout settings for all systems, applications, and devices where sensitive data is accessed (e.g., web portals, cloud platforms, and employee workstations). Ensure timeout policies are uniformly enforced across operating systems, browsers, and applications.
- ***Communicate Policies to Users:*** Notify employees about idle session timeout policies to ensure they understand their purpose and how to comply. Include guidelines on saving work frequently to avoid losing progress when sessions time out.

5.3 Idle Session Timeout

Setting an idle session timeout is a simple yet powerful security measure designed to protect your organization from unauthorized access to sensitive systems and data. An idle session timeout works by automatically logging users out of their accounts or locking their sessions after a specified period of inactivity. This ensures that if a user steps away from their device or forgets to log out, their session cannot be exploited by someone else. Without this safeguard, an unattended session could be a gateway for malicious actors to access sensitive information, manipulate systems, or compromise organizational security.

The risk is particularly significant on shared or public devices, where multiple users may have access. For example, an employee working on a personal laptop at a coffee shop might inadvertently leave a session open, allowing the next person to access their account. Idle session timeouts help mitigate this risk by cutting off access as soon as inactivity is detected, effectively locking out unauthorized users.

Moreover, idle session timeouts encourage a culture of security awareness. Employees and users become more mindful of their digital activities, knowing their access will be automatically revoked after a period of inactivity. This awareness can lead to better habits, such as manually logging out or securing devices when stepping away.

When configuring idle session timeouts, it’s important to strike the right balance between security and user convenience. Setting the timeout period too short could frustrate users, leading to inefficiencies or resistance to the policy. Conversely, setting it too long could leave sessions vulnerable to unauthorized access. Best practices often suggest a timeout period that aligns with the sensitivity of the systems and the typical workflow of users.

Idle session timeouts provide an effective way to enhance a CDFI’s security posture. By automatically ending inactive sessions, the CDFI reduces the risk of unauthorized access, safeguards sensitive data, and ensures that systems remain secure.

What to do:

- ***Determine Timeout Duration:*** Assess the nature of your business processes and determine a suitable idle timeout period (e.g., 5, 10, or 15 minutes of inactivity). Balance security needs with user convenience to avoid overly short timeouts that disrupt productivity. Consider industry standards or regulatory requirements that may mandate specific timeout settings.
- ***Apply Timeout Settings Across All Systems:*** Configure idle session timeout settings for all systems, applications, and devices where sensitive data is accessed (e.g., web portals, cloud platforms, and employee workstations). Ensure timeout policies are uniformly enforced across operating systems, browsers, and applications.
- ***Communicate Policies to Users:*** Notify employees about idle session timeout policies to ensure they understand their purpose and how to comply. Include guidelines on saving work frequently to avoid losing progress when sessions time out.

5.4 Full Disk Encryption

Full disk encryption is a critical security measure that safeguards the information stored on computers and devices by converting data into an unreadable format. This encryption ensures that only authorized users, who have the appropriate decryption key or credentials, can access the data. By securing all the information on a device, encryption provides comprehensive protection against unauthorized access, even if the device itself is compromised.

One of the most significant benefits of full disk encryption is its ability to protect sensitive data in the event of device loss or theft. Whether it’s a misplaced laptop, a stolen tablet, or a lost smartphone, encrypted data remains inaccessible to unauthorized individuals. Without the decryption key, the scrambled data is essentially meaningless, rendering the device's contents useless to anyone attempting to access it unlawfully.

This protection is especially vital for safeguarding sensitive information such as financial records, client details, proprietary business documents, and personal information. For organizations handling sensitive data, a lost or stolen device without encryption can result in severe consequences, including data breaches, financial losses, reputational damage, and violations of privacy obligations. Full disk encryption significantly mitigates these risks by ensuring that data remains secure even when physical security is compromised.

Encryption also provides protection against certain types of cyberattacks, such as boot-level malware and unauthorized data extraction. Since encryption applies to the entire disk, it prevents attackers from accessing files by booting the device from an external drive or using specialized tools to bypass the operating system.

Implementing full disk encryption is particularly important for mobile devices and laptops, which are more likely to be lost or stolen due to their portable nature. CDFIs should also consider encrypting desktop systems, especially in environments where physical access cannot always be controlled.

Full disk encryption is an essential component of a robust data security strategy. It protects sensitive information by making it inaccessible to unauthorized users, even in cases of physical loss or theft. By adopting full disk encryption, CDFIs can confidently safeguard their data, maintain privacy, and uphold the trust of clients, partners, and stakeholders.

What to do:

- ***Choose an Encryption Solution:*** Select a full-disk encryption solution that aligns with your organization’s needs and budget. Third-party solutions for cross-platform compatibility or advanced features.
- ***Enable Encryption on Devices:*** Activate encryption on all devices as part of their setup process. For existing devices, ensure users back up critical data before enabling encryption to prevent data loss. Automate encryption activation using deployment tools or endpoint management solutions.

- ***Verify Encryption Status:*** Check that encryption is active and functioning correctly on all devices. Perform periodic audits to confirm compliance and identify unencrypted devices.
- ***Test Recovery Processes:*** Ensure you have a reliable method to recover data from encrypted drives in case of hardware failure or lost credentials. Test recovery scenarios periodically to validate the effectiveness of your backup and key recovery processes.

6. Technical Controls for the Organization

6.1 Backups

Backups are a cornerstone of cybersecurity and business continuity, designed to protect data from loss, corruption, or unauthorized access resulting from incidents like cyberattacks, hardware failures, natural disasters, or human error. Implementing effective backup practices not only ensures data restoration but also minimizes downtime and disruption to business operations.

A comprehensive backup strategy involves several key elements. First, CDFIs should adopt an automated backup system that regularly creates copies of critical data, applications, and system configurations. To enhance reliability, data should be stored on two different media types with one copy stored offsite or in a secure cloud environment. This diversification protects against localized failures and offers resilience against widespread disruptions.

Regular testing of backup and restoration processes is critical to verify the integrity of the backups and ensure recovery procedures function as expected during an actual incident. This includes simulating various recovery scenarios to identify potential gaps in the process and fine-tune procedures accordingly. Organizations should also maintain a detailed backup schedule that prioritizes the most critical systems and data, ensuring rapid recovery of essential operations when needed.

Beyond the technical aspects, backup strategies should align with the organization's overall risk management plan and compliance requirements.
By prioritizing and maintaining an effective backup strategy, organizations protect their operational integrity, minimize the impact of unforeseen disruptions, and foster long-term resilience in an ever-evolving threat landscape.

What to do:

- ***Determine Backup Requirements***: Using the risk assessment, data map, and asset inventory, identify the critical systems, applications, and data that need to be backed up based on data map and asset inventory.
- ***Determine Continuity and Recovery Objectives***: These should be based on business need and should include maximum acceptable data loss and maximum acceptable downtime.
- ***Select Backup Solution***: Choose a backup strategy that aligns with your organization's needs.
- ***Implement Backup Schedules***: Define the frequency and retention period for backups, considering data sensitivity and business requirements. Example: Daily incremental backups and weekly full backups with a 30-day retention period. Stagger backup timings to avoid performance bottlenecks during business hours.
- ***Test Backups Regularly***: Perform periodic restore tests to ensure backups can be recovered successfully and meet objectives. Validate data integrity and consistency during restore tests.

6.2 Automated Patching

Automated patching enables organizations to quickly and consistently address vulnerabilities in software, applications, and systems. By automating the patch management process, organizations can reduce the time and effort required to deploy updates, ensuring that critical vulnerabilities are addressed promptly and systems remain protected against emerging threats.

Automated patching works by regularly scanning systems to identify outdated software or missing updates and then deploying the necessary patches without requiring manual intervention. This process ensures that systems stay up to date with the latest security fixes, reducing the risk of exploitation by attackers who target unpatched vulnerabilities. One of the key advantages of automated patching is its ability to minimize downtime and disruption. Updates can be scheduled during off-peak hours to ensure business continuity while reducing the risk of human error that often accompanies manual patching processes.

Effective automated patching solutions include centralized management dashboards that provide visibility into patching status across all systems and devices. These tools allow organizations to prioritize updates based on the severity of vulnerabilities and the criticality of affected systems, ensuring that high-risk issues are addressed first.

By implementing automated patching, organizations can significantly enhance their cybersecurity posture, reducing their exposure to threats and ensuring the stability of their systems. This proactive approach not only protects critical assets and data but also saves time and resources, allowing IT and security teams to focus on other strategic initiatives. Ultimately, automated patching is a vital tool for staying ahead of cyber threats and maintaining operational resilience in today’s fast-evolving threat landscape.

What to do:

- ***Assess Patch Management Requirements:*** This will be based on your asset inventory and risk assessment, but should include critical systems, applications, and devices that require patching.
- ***Select an Automated Patching Solution:*** Choose a patch management tool that aligns with your organization's needs.
- ***Establish Patch Deployment Schedules:*** Define maintenance windows for deploying patches to minimize disruption. Configure the automated patching tool to deploy patches during off-peak hours.
- ***Test Patches Before Deployment:*** Create a testing environment that mirrors production systems to validate patches. Test for compatibility issues, application stability, and system performance.

6.3 Vulnerability Scanning

Vulnerability scanning identifies weaknesses in your systems, networks, and applications that attackers could exploit. By regularly conducting scans, organizations can proactively detect and address security gaps such as outdated software, unpatched vulnerabilities, misconfigurations, and other potential entry points for malicious actors. This proactive approach helps reduce the attack surface and strengthens overall security.

A comprehensive vulnerability scanning process involves using automated tools, which compare system configurations and software versions against known vulnerabilities, providing detailed reports that highlight potential risks and their severity. By prioritizing these vulnerabilities based on risk level, organizations can allocate resources to address the most critical issues first.

Regular scanning is essential for staying ahead of threats in an ever-changing landscape. Attackers constantly evolve their tactics, and new vulnerabilities are discovered daily. Routine scans ensure that organizations remain aware of emerging risks and can promptly address them before they are exploited. Scheduling scans at regular intervals—such as weekly, monthly, or after significant system changes—helps maintain a consistent security posture.

Incorporating vulnerability scanning into a CDFI’s security strategy enables a proactive defense against threats. It helps reduce the likelihood of successful attacks, limits potential damage, and fosters confidence among stakeholders. By addressing vulnerabilities before they can be exploited, CDFIs can maintain a strong security posture and better protect their assets, data, and reputation.

What to do:

- ***Choose a Scanning Tool:*** Select a vulnerability scanner that fits your organization’s size and needs, such as Nessus or Qualys.
- ***Perform Regular Scans:*** Schedule scans on a consistent basis to identify new vulnerabilities as your systems change.
- ***Prioritize Results:*** Review scan reports and the risk assessment to prioritize high-risk vulnerabilities that need immediate attention.
- ***Patch and Mitigate:*** Apply patches or configuration changes to address identified vulnerabilities promptly
- ***Document and Track Progress:*** Keep a record of scans, findings, and actions taken to ensure continuous improvement in your security efforts.

6.4 Audit Logging

Audit logging provides a detailed and continuous record of important activities within your systems. This includes logging actions such as user logins, data modifications, file accesses, configuration changes, and security events. These logs create a chronological history of system activity, helping CDFIs detect unusual behavior, investigate incidents, and meet compliance obligations, if any apply.

By enabling audit logging, CDFI’s can monitor user and system actions in real time, identifying potential threats such as unauthorized access, suspicious activity, or insider misuse. Logs serve as a critical source of evidence, enabling security teams to trace the origin and scope of incidents during investigations. This can significantly reduce response times and minimize the impact of breaches or system misconfigurations.

To maximize the effectiveness of audit logging, organizations should implement centralized logging systems that collect and store logs from all critical systems, networks, and applications. Using tools such as Security Information and Event Management (SIEM) solutions, logs can be aggregated, analyzed, and correlated to detect patterns or anomalies that might indicate security risks. Automation and alerting capabilities within these tools can help organizations quickly identify and respond to threats.

Additionally, log retention policies should be established based on the CDFI's operational needs and any regulatory requirements. Ensuring that logs are stored securely and are tamper-proof is critical to maintaining their integrity and reliability. Access to logs should be restricted to authorized personnel only, with controls in place to prevent unauthorized modifications or deletions.

Audit logging not only enhances security but also fosters a culture of accountability and transparency. By providing clear visibility into system activity, CDFIs can ensure that users follow established policies and procedures. This level of oversight helps maintain trust among stakeholders, strengthens the organization’s security posture, and ensures long-term operational resilience.

What to do:

- ***Define Audit Logging Requirements:*** Using the asset inventory and risk assessment, identify key systems, applications, and processes that require logging.
- ***Select Logging Tools:*** Consider centralized logging solutions such as a Security Information and Event Management system.
- ***Enable Regular Log Reviews:*** Establish a schedule for reviewing logs to identify anomalies or suspicious activities. Consider automating log analysis for routine events while focusing manual reviews on flagged or high-risk incidents.
- ***Conduct Log Retention and Archiving:*** Set retention based on business needs and any compliance requirements (ie 1 year or 7 years).

7. The Human Element

The human element is one of the most critical factors in maintaining a strong security posture. While technology provides the tools and systems to protect data and networks, it is the actions, decisions, and behavior of employees, contractors, and other users that often determine the effectiveness of a security strategy. Cybercriminals are adept at exploiting human vulnerabilities, taking advantage of social engineering tactics like phishing, spear-phishing, and pretexting, as well as weaknesses such as poor password management or the accidental sharing of sensitive information.

Human error can manifest in numerous ways, from employees inadvertently clicking on malicious links in emails to failing to follow proper data handling protocols. For example, weak or reused passwords make it easier for attackers to gain unauthorized access to systems. Similarly, poor judgment, such as neglecting to report suspicious activity or bypassing security measures to save time, can leave critical systems and data exposed to attacks.

While technology remains a cornerstone of any security strategy, the human element is equally crucial. By fostering a culture of security awareness, providing regular training, and implementing clear policies, organizations can minimize risks associated with the human element and empower their teams to be proactive in identifying and preventing potential threats.

7. The Human Element Controls:

7.1 Security & Privacy Training

7.2 Password Management

7.3 Secure File Sharing

7.4 Background Screening

7.1 Security & Privacy Training

Security and privacy training equips employees with the knowledge and skills needed to recognize and mitigate potential threats. Through regular training, employees learn to identify risks such as phishing emails, malicious links, social engineering tactics, and other common attack methods that could jeopardize the organization's security. This proactive approach not only helps protect sensitive data but also empowers employees to act as the first line of defense against cyber threats.

Comprehensive security training programs cover essential topics, including how to create strong passwords, recognize suspicious activity, properly handle sensitive information, and respond appropriately to potential incidents. By understanding these principles, employees can minimize risky behaviors, such as clicking on unsafe links or sharing credentials, which often serve as entry points for attackers.

To maximize effectiveness, training should be tailored to the CDFI's specific risks, determined during the risk assessment, and updated regularly to reflect the latest threat landscape. Interactive elements such as simulations of phishing attacks and real-world scenarios can help reinforce key concepts, ensuring that lessons are practical and memorable. Providing additional role-specific training for employees in high-risk positions, such as those handling financial transactions or access to sensitive systems, can further reduce vulnerabilities.

Security training also plays a critical role in fostering a culture of awareness and accountability throughout the CDFI. When employees understand their role in maintaining security, they are more likely to report suspicious activities, follow policies, and support best practices. This collective vigilance strengthens the overall security posture and reduces the likelihood of successful attacks.

By investing in ongoing security and privacy training, organizations can significantly reduce the risk of human error, safeguard critical data, and build resilience against evolving cyber threats. This commitment to education enhances operational security, protects the organization's reputation, and ensures long-term success in an increasingly digital world.

What to do:

- ***Identify Training Needs:*** Assess your organization's specific cybersecurity and privacy risks. Identify roles that require additional role-based training, such as IT administrators, financial staff, and executive management.
- ***Determine a Training Cadence:*** Define mandatory training sessions, frequency, and key topics. Include new hire orientation and training.
- ***Select Learning Management System:*** The LMS should record attendance for live sessions, monitor completion of online training modules, and generate reports to identify non-compliance and track progress.
- ***Incorporate Simulated Attacks and Exercises:*** Conduct phishing simulations to test awareness and readiness.
- ***Track Attendance and Completion:*** Monitor completion of training modules. Generate reports to identify non-compliance and track progress. Specify consequences for non-compliance with training requirements.

7.2 Password Management

Password managers provide a secure and efficient way to store, manage, and access passwords. They enable users to create and use strong, unique passwords for every account without the need to remember them all, significantly reducing the risks associated with weak or reused credentials. By simplifying password management, password managers help protect accounts from unauthorized access and prevent breaches caused by compromised passwords.

A password manager securely encrypts all stored passwords, ensuring they remain protected even if the password manager itself is targeted. These tools often include features like random password generation, which helps users create complex, hard-to-guess passwords that are more resistant to brute force attacks. Additionally, password managers offer auto-fill capabilities, saving time and reducing the likelihood of errors when entering credentials or entering credentials into copycat websites designed to learn credentials through phishing.

For CDFIs, implementing a password manager is a strategic way to enhance overall security. Employees gain a streamlined way to manage their passwords while adhering to security best practices, such as using unique passwords for every account and avoiding unsafe storage methods like spreadsheets or sticky notes. Centralized administration features in enterprise password managers allow IT teams to enforce policies, such as password complexity requirements, and monitor usage to ensure compliance.

Beyond enhancing security, password managers improve user productivity by reducing login friction and eliminating the frustration of forgotten passwords. Employees can focus on their tasks without being bogged down by password-related challenges, while organizations benefit from fewer help desk requests for password resets.

By adopting a password manager, CDFIs can reduce the likelihood of breaches caused by weak, reused, or stolen credentials. This proactive measure strengthens security, fosters a culture of responsibility among employees, and demonstrates the organization’s commitment to protecting its assets and data in an increasingly threat-prone digital environment.

What to do:

- ***Choose a Password Manager:*** Select a password manager that suits your organization’s needs.
- ***Train Employees:*** Provide training on how to use the password manager effectively and safely
- ***Mandate Password Manager Use:*** Require all employees to store and manage their passwords exclusively in the password manager.

7.3 Background Screening

Background screening ensures that employees, contractors, and other personnel meet the necessary standards of trustworthiness and reliability. By verifying the history, qualifications, and credentials of individuals before they are granted access to sensitive systems or data, background screening helps reduce the risk of insider threats, fraud, and negligence.

A comprehensive background screening process typically includes checks for employment history, education verification, criminal records, and credit reports. These measures ensure that candidates are not only qualified for their positions but also free from past actions or behaviors that could pose a risk to the organization.

For CDFIs, background screening is particularly critical for roles that involve access to sensitive information and financial transactions. By identifying potential red flags during the hiring process, organizations can make informed decisions and mitigate risks before they materialize. This proactive approach reduces the likelihood of hiring individuals who may engage in malicious or unethical behavior.

Incorporating background screening into CDFI hiring and onboarding processes enhances security, protects organizational assets, and fosters a culture of trust and accountability. It reassures stakeholders, clients, and customers that the organization is committed to maintaining the highest standards of integrity and professionalism. By identifying and addressing risks early, background screening serves as a critical layer of defense in a CDFI’s overall security strategy.

What to do:

- ***Define the Scope of Screening:*** Identify roles requiring background checks.
- ***Select a Screening Provider:*** Select a reliable and certified background screening service. Verify the provider’s compliance with applicable data privacy and security standards.
- ***Conduct Role-Specific Checks:*** Tailor screenings to the role’s risk level and responsibilities. Extend screening policies to any contractors with access to sensitive systems or financial data.
- ***Integrate Background Screening into Onboarding:*** Ensure screenings are completed before granting access to sensitive systems or data. Re-Screen Employees Periodically. Establish a process to document and verify completed screenings during onboarding.
- ***Establish Clear Criteria for Decision-Making:*** Define acceptable and unacceptable findings for specific roles. Use consistent standards to ensure fair and unbiased hiring decisions.
- ***Train Hiring Teams:*** Educate relevant staff on interpreting background check results, legal obligations and anti-discrimination practices, and handling sensitive candidate information with confidentiality.

8. Administrative Controls

Standardizing administrative procedures is a vital strategy for ensuring consistency, efficiency, and security. By establishing clear, uniform processes for tasks such as financial management and vendor relationships, CDFIs can minimize risks, improve accountability, and maintain compliance with regulatory requirements. This is especially important in sensitive areas like secure financial procedures and vendor management, where robust protocols are essential for safeguarding assets and protecting against fraud or mismanagement.

In financial procedures, standardization helps prevent errors, discrepancies, and fraud by ensuring that all transactions are processed according to a consistent, secure set of guidelines. These procedures may include controls such as segregation of duties, approval workflows, and regular audits. By clearly defining roles and responsibilities, organizations can reduce the risk of unauthorized access to financial systems and prevent conflicts of interest that could lead to fraudulent activities. Additionally, financial procedures should mandate the use of secure payment systems, encryption for sensitive data, and timely reconciliation of accounts to ensure financial integrity and transparency.

Vendor management is another critical area where standardizing procedures enhances security and operational efficiency. A standardized vendor management process ensures that all third-party relationships are consistently evaluated, monitored, and managed according to a clear set of criteria. This includes verifying the security and financial stability of potential vendors, negotiating contracts with clear terms, and regularly assessing vendor performance to ensure compliance with agreed-upon standards. By implementing a formalized vendor approval process and requiring vendors to meet security and compliance requirements, organizations can minimize risks associated with third-party breaches, financial instability, or unethical practices.

To ensure the success of standardized administrative procedures, organizations should provide training for employees and vendors on the proper execution of these processes. Clear documentation of procedures, regular audits, and continuous improvement efforts are also essential for maintaining the effectiveness and security of the system.
Ultimately, standardizing administrative procedures creates a structured, secure environment that reduces operational risks, ensures compliance, and improves overall efficiency. By implementing secure financial procedures and a robust vendor management system, organizations can protect their assets, maintain trust with stakeholders, and promote a culture of accountability and transparency.

8. Administrative Procedures:

8.1 Financial Transaction Procedures

8.2 Vendor Management

8.3 Account Granting & Revokation

8.1 Financial Transaction Procedures

A standard approval process for financial transactions is a critical safeguard for any CDFI, ensuring that financial transactions are properly reviewed and authorized before they are executed. By introducing these extra checks, the approval process not only prevents mistakes and fraud but also strengthens overall financial accountability, making it more difficult for unauthorized spending or errors to slip through the cracks.

The standard approval process typically involves several key steps. First, there should be clear guidelines on who has the authority to approve different types of transactions, depending on their size and nature. For example, smaller, routine purchases may require only a manager's approval, while larger or more complex transactions, such as capital expenditures or contracts, may require senior leadership or board-level approval. By defining approval hierarchies and thresholds, organizations ensure that transactions are always reviewed by the appropriate individuals.

Another critical aspect of the approval process is documentation. Each transaction should be accompanied by sufficient supporting information. This documentation serves as a record of the decision-making process, helping to maintain transparency and traceability in financial operations. It also allows for easy audits, as the documentation will be available to verify that the appropriate steps were followed and that the funds were allocated properly.

The approval process also plays an essential role in fraud prevention. By requiring multiple levels of authorization for significant transactions, CDFIs reduce the risk of a single individual making a mistake. For instance, a dual-approval system can require two individuals to sign off on a payment, which makes it more difficult for fraudulent transactions to go unnoticed. Additionally, by clearly defining roles and responsibilities, organizations can prevent conflicts of interest and ensure that no single person has too much control over the financial decision-making process.

In summary, a standard approval process for financial transactions is an indispensable tool for any CDFI, ensuring that payments and financial activities are properly vetted before they are carried out. By requiring appropriate oversight, documentation, and multiple layers of authorization, CDFIs can reduce the risk of fraud, minimize errors, maintain financial discipline, and protect their financial integrity. This structured approach not only helps safeguard an organization's funds but also contributes to transparency, accountability, and long-term success.

What to do:

- ***Define Approval Hierarchies and Thresholds:*** Document who can approve different types and amounts of financial transactions. For example, purchases under $500 may need approval from a manager, while transactions between $500 and $10,000 may need approval from both a manager and a director, and while larger expenditures or contractual agreements may require approval from the Executive Director or Board.
- ***Separate Financial Accounts:*** Consider using a dedicated account for outgoing payments, a separate dedicated account for receiving payments, and another dedicated account to hold all funds. Keep operating funds, grant funds, and reserve funds separated so that unauthorized or mistaken transactions are less likely to affect all funds at once. Always move funds as soon as possible from the receiving account. Only move funds in the outgoing account when all necessary approvals are completed. Never share the holding account or outgoing account details

- ***Use a Standardized Intake Form for All Requests:*** Create a standardized intake form for all requests to transfer money. Ensure access to the form is available only to people in your CDFI and that all approvers are notified when a request is submitted.
- ***Document the Approval Process:*** Decide how approvals will be managed and recorded. Consider a change management or ticketing system to manage approvals. Store all approvals and supporting documents in a central repository to maintain an audit trail.

- ***Require Multiple Approvals for Outgoing Funds:*** Ensure that for any transaction sending CDFI funds externally, at least two people must sign off before funds are released. After the initial approval from a manager, the request might automatically go to a second approver (like a director or the Executive Director) for final sign-off before the funds are released.
- ***Conduct Regular Audits and Reviews:*** Periodically review intake form responses and related documentation to ensure that the financial transaction procedures are being followed. Monitor whether approval thresholds are respected and verify that the correct supporting documents are attached.

8.2 Vendor Management

Vendor management is a crucial process for organizations to effectively and securely manage their relationships with third-party suppliers, contractors, and service providers. A standardized vendor management process helps ensure that all vendor interactions, from selection to ongoing performance monitoring, are conducted systematically and consistently. By establishing clear guidelines and procedures for managing vendors, organizations can mitigate third-party risk.

The vendor management process begins with vendor selection, ensuring that potential suppliers meet the security requirements. During the selection process, CDFIs should rank vendors by security and business requirements. This helps organizations identify reliable, trustworthy partners who can meet their needs without exposing the organization to unnecessary risks. Regular monitoring is also essential, as security controls and the organization's needs can change.

In the context of vendor management, security is a top priority. As vendors often have access to sensitive organizational data and systems, it is crucial to establish strong security controls and protocols to mitigate risks such as unauthorized access or data breaches. CDFIs should seek vendors that adhere to security best practices, such as using multi-factor authentication, encryption for data transmission, and conducting regular security audits.

A well-structured vendor management program also includes a contingency plan for dealing with potential issues, such as vendor failure, service disruptions, or non-compliance. This might involve identifying backup vendors, creating exit strategies, or establishing protocols for quickly addressing any disruptions in service. Having a contingency plan in place helps ensure business continuity and minimizes the impact of any vendor-related challenges.

Ultimately, effective vendor management strengthens the CDFI's security and operational efficiency. By maintaining strong relationships with reliable vendors and continuously monitoring them, organizations can mitigate risks, maintain high standards of service, and ensure that third-party partnerships contribute positively to CDFI's success. A consistent and well-defined vendor management process helps protect the CDFI's interests, safeguard sensitive data, and support long-term business goals.

What to do:

- ***Identify and Categorize Vendors:*** Create a comprehensive list of all vendors your organization works with and categorize based on their role and access to sensitive data or systems.
- ***Conduct Vendor Risk Assessments:*** Evaluate each vendor's risk level based on the data sensitivity or system access involved and the quality of the vendor's security controls.
- ***Integrate Security and Privacy Requirements into Contracts:*** Whenever possible, include clauses for data protection and confidentiality, security controls and breach notification obligations, and right-to-audit provisions. Review contracts regularly to ensure they reflect current risks and requirements.
- ***Maintain a Vendor Risk Register:*** Create a centralized record of all vendors and risk levels.
- ***Integrate Risk Assessment into Decision-Making:*** Use the vendor risk register to prioritize actions and track risk management progress.

8.3 Account Granting & Revocation

Managing user accounts through standardized processes for granting, revoking, and reviewing access ensures that only authorized individuals have access to the systems and data they need while minimizing the risks associated with outdated, excessive, or inappropriate access. By implementing a structured approach to account management, organizations can safeguard sensitive information, reduce insider threats, and maintain compliance with regulatory requirements.

Granting access should begin with a clear, formalized process to ensure accounts are only created for legitimate users who require specific permissions to perform their roles. This involves verifying the user's identity, defining their job responsibilities, and assigning the appropriate access based on the principle of least privilege. The principle of least privilege ensures that users are granted only the minimum level of access necessary to perform their duties, thereby reducing the risk of unauthorized activity or accidental exposure of sensitive data. Documentation of all access requests and approvals should also be maintained for accountability and future auditing.

Revoking access is equally critical, as it ensures that former employees, contractors, or partners can no longer access systems and data once their association with the organization ends or their role changes. A standardized offboarding process should include immediate deactivation of accounts when a user departs or transitions to a role with different access requirements. This reduces the risk of unauthorized access, which could lead to data breaches or misuse of resources.

When an employee takes on a new role, access should be revoked as if they were leaving the organization. This step is crucial to prevent unauthorized access to systems or data outside the scope of their new responsibilities. Access should then be granted anew based on the employee’s new role.

Periodic reviews of all active accounts are also vital. These reviews ensure that access remains appropriate and aligns with current job responsibilities. These reviews help identify and address excessive permissions, dormant accounts, or accounts that no longer have a valid business justification. Automated tools can be used to generate reports detailing account activity, last login times, and permissions, making it easier to identify discrepancies or potential risks.

During reviews, particular attention should be paid to privileged accounts, as they often have elevated access to critical systems and data. Any unnecessary or unused privileged accounts should be downgraded or deactivated to prevent misuse. Additionally, cross-referencing user roles with their access permissions ensures that no discrepancies exist and that users only have access to what they require.

What to do:

- ***Create Account Change Request Process:*** Require written or documented requests for account creation, revocation, or status change. Require manager or supervisor approval and justification for account access. Create a standard form or digital workflow for account requests.
- ***Establish Timely Account Revocation Procedures:*** As part of the offboarding process for departing employees, contractors, or vendors, disable accounts within a defined timeframe, such as immediately or within 24 hours of departure. Confirm that all access to systems, applications, and third-party platforms is revoked.

- ***Implement Idle Account Monitoring and Cleanup:*** Identify and disable dormant accounts after a set period of inactivity (e.g., 90 days). Notify users before account deactivation and allow reactivation if access is still needed.
- ***Conduct Regular Account Reviews:*** Schedule periodic reviews (e.g., quarterly or annually) to verify: Active accounts are still necessary. Permissions match current roles and responsibilities. Involve managers and system owners in the review process.
- ***Maintain detailed records:*** Record account requests and approvals, permissions granted and revoked, and results of periodic reviews.

About Us

African American Alliance of CDFI CEOs

The African American Alliance of CDFI CEOs is a membership-driven intermediary organization that aims to build the capacity of member organizations; build bridges to economic stability, well being, and wealth for Black individuals, families, and communities; and build power in Black communities by challenging and influencing financial sectors to operate more equitably.

Learn more at AAACDFI.org.

ZenPrivata

ZenPrivata combines an advanced platform and expert consulting to bring Zen to your privacy/cybersecurity program. We make it simple. Quickstart helps you build your privacy program in under an hour and Universal Compliance helps simplify and manage compliance.

Learn more at ZenPrivata.com or contact us directly at Hello@ZenPrivata.com.