THE CRITICAL FOUNDATION OF MANAGING ACCESS TO *Banking Systems*

FINOSEC

In today's evolving financial technological landscape, financial institutions face numerous challenges in managing system access and ensuring robust cybersecurity measures. Legacy system reporting is archaic, complicated, and it is labor intensive to perform reviews.   At the same time, the complexity of environments is increasing with API access and cloud solutions.   and complicated, and performing reviews is labor-intensive. At the same time, API access and cloud solutions are increasing the complexity of environments. There are major risks associated with unmonitored and unmanaged systems. This makes it imperative to maintain a comprehensive inventory of every system accessed by employees and vendors.

Why It's Important to Know Every System for Every Employee

1. **Visibility and Control**
    - Financial institutions often struggle with visibility over all systems within their organization. Shadow IT, or the use of unauthorized applications, further exacerbates this issue by introducing security vulnerabilities that are difficult to detect and manage. With the proliferation of cloud solutions, IT no longer has complete control of what systems your employees use, but the oversight and governance of access remains.
2. **Compliance and Regulatory Requirements**
    - The FFIEC with the Authentication Guidance and key findings in examinations, are requiring financial institutions to maintain detailed records of all systems, access points, and manage to least privilege. Failure to comply with these requirements has resulted in formal actions and write ups.
3. **Risk Management**
    - Without a thorough understanding of all systems, institutions are at risk of exposure to cyber threats. System access is one of the best controls to prevent data breaches, financial losses, and regulatory actions.
4. **Efficiency in Access Management**
    - Managing user access across a complex IT environment can be a complicated and labor intensive task. It is not uncommon for legacy banking applications to have reports that are in unstructured text or pdf reporting with hundreds if not thousands of pages of access data. Even with these barriers, financial institutions must ensure that employees have the appropriate level of access to perform their job functions without compromising security.

How does a System Inventory (or System Map) help address these challenges?

A comprehensive system inventory is essential for maintaining security and governance within any organization. It serves as the foundation for effective risk management by providing the necessary visibility and control over all systems and access points. This detailed inventory enables organizations to quantify and manage risks accurately, implement access policies based on system risk, and ensure that access is appropriately reviewed and governed.

By documenting all systems and system access, institutions can demonstrate compliance with regulatory standards, preparing them thoroughly for external examinations and reducing the risk of non-compliance. Additionally, a well-maintained system inventory allows for the identification of vulnerabilities and potential points of failure, enabling implementation of security controls to mitigate risks associated with unauthorized access and data breaches.

Most importantly, it lays the foundation that employees have the necessary permissions to perform their roles effectively while adhering to the principle of least privilege, thereby minimizing the risk of internal threats and enhancing overall security posture of the institution.

Steps to Enhance Your System Inventory: A Guide for Cybersecurity Governance

These steps will assist you in creating, or validating that your system inventory has the right details.   Each of these steps are data that you want to make sure you have documented in the system map.

1. System Inventory (Function and Purpose)

- Objective: Catalog all systems and understand their specific functions within the organization.
- Action Steps:
  - List all implemented systems and define their roles and functions.
  - Break down the systems by department or functional area, ie, loans, teller, deposit, online banking, wire transfer and payments, etc.
  - Assess how each system contributes to your operational risk and document the risks associated with them. Some examples of these risks include systems that have access to non public and customer information, can perform financial transactions (debits and credits to customer accounts), and related to financial reporting (especially important for FDICIA and SOX compliance)
  - Schedule regular reviews to validate and update the system inventory.

2. Location

- Objective: Determine the locations of your systems to assess their security needs and compliance requirements.
- Action Steps:
  - Identify whether each system is in-house, co-located, cloud-based, or a physical asset.
  - Document the exact location of each system, understanding that location impacts risk levels and security strategies.
  - In-House: Systems located within your institution's physical premises.
  - Co-Lo (Co-location): Systems housed at a third-party data center.
  - Cloud Systems: Services and applications hosted online (ie, Office 365, Hosted Core Processing).
  - Physical Asset: Physical devices used in operations, such as devices for instant debit card issuance.

3. **Third-Party Access and OversightVendor Documentation**
    - Objective: Identify the third-partiesvendors involved with each systems and understand their impact on your cybersecurity posture.
    - Action Steps:
        - Document which vendors third-parties are associated with each system, highlighting those with access to PII-containing systems
        - Document individual login access and single sign sign-on capabilities for the systems
        - Review vendor SOC reports and highlight user entity controls that are the institution’s responsibility for managing access to the systems.
4. **Access Management**
    - Objective: Document what systems have individual logins to ensure security and compliance with regulatory standards.
    - Action Steps:
        - Identify which systems require specific user accounts
        - Develop a quick-reference list of systems with accounts that have access to each system
5. **Managing System Access**
    - Objective: Implement access control reporting to document who can access systems and what they can do with that access.
    - Action Steps:
        - Maintain a comprehensive inventory of all systems requiring user access reviews.
        - Define the frequency of the access reviews that are needed based on the system risk
        - Validate the process for addressing access risk when adding new systems
        - Document the review process for system access risk
6. **Manager and Department Head Validation**
    - Objective: Ensure that all systems and access permissions align with the actual needs and responsibilities of each department.
    - Action Steps:
        - Implement a validation process where managers and department heads review and approve the system inventory specific to their departments.

7. System Ownership

- Objective: Clearly define who is responsible for the operation and oversight of each system.
- Action Steps:
  - Assign a Business Owner responsible for the strategic management of each system. Tip: Think about who signs the contract.
  - Designate a System Owner (or System Administrator), who may be an internal employee, responsible for the daily operational management of the system.

If navigating the complexities of system inventory seems daunting, our team is here to help. We have helped hundreds of intuitions in creating and maintaining a detailed system inventory that enhances your institution’s cybersecurity governance. Reach out to our team today at info@finosec.com, and let us assist you in simplifying the steps of documenting your systems and safeguarding your operations.