Data Governance

Thursday, August 15, 2024 2:35 PM

Stmt 19.1: CORE+ Policy or Program Established

- **Documentation Review**
  - Obtain and review the data management policy or program documentation.
  - Verify the policy covers identification, classification, secure handling, retention, and disposal of data.
  - Confirm the policy is formally approved by relevant stakeholders (e.g., board, senior management).
- **Interviews and Observations**
  - Interview personnel responsible for data management to confirm understanding of the policy.
  - Observe adherence to the policy in daily operations.

Stmt 19.2: Data Inventory Established

- **Documentation Review**
  - Obtain the data inventory list.
  - Verify it includes all types of data managed by the organization.
- **Accuracy Check**
  - Cross-check the inventory list with actual data sources for completeness.
- **Update Process**
  - Review the process for updating the inventory and confirm it is documented and followed.

Stmt 19.3: Data Access List Established

- **Documentation Review**
  - Obtain the data access list.
  - Verify it includes access permissions, roles, and responsibilities.
- **Access Controls**
  - Check the process for reviewing and updating access controls.
- **Interviews**
  - Interview personnel responsible for access control management.

Stmt 19.4: Data Retention Enforced

- **Documentation Review**
  - Obtain the data retention policy.
  - Verify it defines retention periods for various data types.
- **Implementation Check**
  - Review records to confirm data is retained according to the policy.
- **Audit Logs**
  - Inspect audit logs or reports to verify data retention compliance.

Stmt 19.5: Data Disposed of in Accordance with Its Sensitivity

- **Documentation Review**
  - Obtain procedures for data disposal.
  - Verify procedures cover data sensitivity levels.
- **Disposal Records**
  - Check records of data disposal to ensure compliance with sensitivity-based procedures.
- **Interviews**
  - Interview staff involved in data disposal.

Stmt 19.6: Data Encrypted on End-User Devices

- **Policy Review**
  - Obtain the encryption policy for end-user devices.
- **Implementation Check**
  - Verify that encryption is enabled on a sample of end-user devices.
- **Device Testing**
  - Test devices to confirm encryption functionality.

Stmt 19.7: Sensitive Data Encrypted at Rest and in Transit

- **Documentation Review**
  - Obtain encryption standards for data at rest and in transit.
- **Implementation Check**
  - Verify that sensitive data is encrypted both at rest and in transit.
- **Audit Logs**
  - Review encryption logs or reports for compliance.

Stmt 19.8: Remote Wipe Process in Place

- **Policy Review**
    - Obtain the remote wipe policy for portable devices.
- **Functionality Testing**
    - Test the remote wipe process on a sample of company-owned portable devices.
- **Coverage Check**
    - Verify that all portable devices are covered by the policy.

Stmt 19.9: Data Management Controls for Safeguarding Data

- **Documentation Review**
    - Obtain controls documentation for both physical and digital data.
- **Safeguard Inspection**
    - Inspect physical data storage areas and digital systems.
- **Control Verification**
    - Verify the presence and effectiveness of safeguards.

Stmt 19.10: Documentation of Data Types, Owners, and Purpose

- **Documentation Review**
    - Obtain documentation on data types, owners, users, and report purposes.
- **Accuracy Check**
    - Cross-check the documentation with actual data records and stakeholders.

Stmt 19.11: Controlling Non-Masked Data in Non-Production Environments

- **Process Review**
    - Obtain and review processes for controlling non-masked data in non-production environments.
- **Implementation Check**
    - Verify that non-masked data is not used or stored in non-production environments.
- **Controls Testing**
    - Conduct tests to confirm the effectiveness of controls.

Stmt 19.12: Data Removal or Destruction in Data Analytics Tools

- **Process Review**
    - Obtain and review processes for removing or destroying data from analytics tools.
- **Compliance Check**
    - Verify that data is removed or destroyed as per the defined processes.

Stmt 19.13: Compliance with Applicable Laws and Regulations

- **Process Review**
    - Identify and review data analytics processes for compliance with laws (e.g., Bank Secrecy Act).
- **Compliance Check**
    - Verify that data analytics practices adhere to applicable regulations.

Stmt 19.14: Data Oversight Committee Composition

- **Documentation Review**
    - Obtain and review documentation on the data oversight committee’s composition.
- **Interviews**
    - Interview committee members to confirm their roles and responsibilities.

Stmt 19.15: Oversight Committee Review of Metrics

- **Metrics Review**
    - Obtain and review metrics or reports that demonstrate the information security program's effectiveness.
- **Review Process Check**
    - Verify that the oversight committee regularly reviews these metrics.

General Tasks

- **Document Findings**
    - Maintain detailed records of all audit activities, including evidence, observations, and interviews.
- **Prepare Report**
    - Compile a comprehensive audit report summarizing compliance status and any areas needing improvement.
- **Develop Action Plan**
    - Create an action plan to address any identified gaps or non-compliance issues.
- **Schedule Follow-Up**
    - Plan follow-up reviews as necessary to ensure issues are resolved.

Tools

Thursday, August 15, 2024 2:42 PM

**1. Audit Management Tools

- **TeamMate**
  - **Features**: Audit planning, execution, reporting, and tracking.
  - **Benefits**: Centralized platform for managing audit workflows and documentation.
- **AuditBoard**
  - **Features**: Risk management, audit planning, reporting, and compliance tracking.
  - **Benefits**: Comprehensive platform with intuitive dashboards and integration capabilities.
- **ACL (Audit Command Language)**
  - **Features**: Data analysis, audit automation, and visualization.
  - **Benefits**: Powerful for data analysis and automating audit tests.
- **Galvanize (formerly ACL)**
  - **Features**: Risk management, audit management, and compliance.
  - **Benefits**: Advanced data analysis and automation capabilities.

**2. Data Management and Inventory Tools

- **Microsoft Azure**
  - **Features**: Data storage, management, and analytics.
  - **Benefits**: Scalable cloud platform with robust data management capabilities.
- **AWS IAM (Identity and Access Management)**
  - **Features**: Access control and management for AWS resources.
  - **Benefits**: Comprehensive tools for managing user access and permissions.
- **ServiceNow**
  - **Features**: IT service management, asset management, and compliance tracking.
  - **Benefits**: Integrated platform for managing IT assets and data.

**3. Encryption and Security Tools

- **BitLocker (Windows)**
  - **Features**: Full disk encryption for Windows devices.
  - **Benefits**: Ensures data encryption on end-user devices.
- **VeraCrypt**
  - **Features**: Disk encryption software.
  - **Benefits**: Open-source solution for encrypting data at rest.
- **McAfee Complete Data Protection**
  - **Features**: Encryption, data loss prevention, and compliance.
  - **Benefits**: Comprehensive data protection solution with encryption and remote wipe features.
- **Symantec Endpoint Protection**
  - **Features**: Endpoint protection, encryption, and data loss prevention.
  - **Benefits**: Robust protection for endpoint devices with encryption capabilities.

**4. Remote Wipe and Device Management Tools

- **MobileIron (now part of Ivanti)**
  - **Features**: Mobile device management, remote wipe, and security.
  - **Benefits**: Manages and secures mobile devices, including remote wipe functionality.
- **Jamf Pro**
  - **Features**: Apple device management, including remote wipe and encryption.
  - **Benefits**: Tailored for managing Apple devices with remote wipe capabilities.
- **Microsoft Intune**
  - **Features**: Mobile device and application management, including remote wipe.
  - **Benefits**: Integrated with Microsoft ecosystem for comprehensive device management.

**5. Database and Analytics Platforms

- **SQL Server**
  - **Features**: Relational database management and analytics.
  - **Benefits**: Comprehensive database platform with advanced analytics features.
- **Oracle Database**
  - **Features**: Enterprise database with strong data management and analytics.
  - **Benefits**: High-performance database with extensive analytics capabilities.
- **Tableau**
  - **Features**: Data visualization and reporting.
  - **Benefits**: Provides interactive dashboards and reports for data analysis.
- **Power BI (Microsoft)**
  - **Features**: Business analytics and data visualization.
  - **Benefits**: Integrates with various data sources for interactive reporting and visualization.

**6. Compliance and Risk Management Tools

- **OneTrust**
  - **Features**: Privacy management, compliance, and risk management.
  - **Benefits**: Helps manage data privacy compliance and risk assessments.
- **MetricStream**
  - **Features**: Governance, risk, and compliance management.
  - **Benefits**: Comprehensive platform for managing compliance and risk.
- **RSA Archer**
  - **Features**: Risk management, compliance tracking, and audit management.
  - **Benefits**: Provides a robust framework for managing risks and compliance.

**7. Automated Scripting and Integration Tools

- **Python**
  - **Features**: Scripting and automation.
  - **Benefits**: Versatile programming language for writing custom scripts for data collection and validation.
- **PowerShell**
  - **Features**: Automation for Windows environments.
  - **Benefits**: Useful for automating administrative tasks and data extraction on Windows systems.
- **Zapier**
  - **Features**: Workflow automation and integration.
  - **Benefits**: Connects various applications and automates workflows without coding.
- **Integromat (now Make)**
  - **Features**: Workflow automation and integration.
  - **Benefits**: Automates processes by integrating multiple tools and services.

**8. Document Management and Reporting Tools

- **Adobe Acrobat**
  - **Features**: Document creation, editing, and PDF management.
  - **Benefits**: Useful for creating and managing audit reports and documentation.
- **Microsoft Office 365**
  - **Features**: Document management, spreadsheets, and presentations.
  - **Benefits**: Tools like Excel and Word are useful for documenting audit findings and generating reports.

**9. Task Management and Collaboration Tools

- **Asana**
  - **Features**: Task management and project tracking.
  - **Benefits**: Helps manage and track audit tasks and follow-up actions.
- **Trello**
  - **Features**: Kanban-style task management.
  - **Benefits**: Visual task management and tracking for audit activities.
- **Slack**
  - **Features**: Team communication and collaboration.
  - **Benefits**: Facilitates communication and collaboration among audit team members.

**10. Security and Compliance Scanners

- **Nessus**
  - **Features**: Vulnerability scanning and assessment.
  - **Benefits**: Identifies security vulnerabilities and compliance issues.
- **Qualys**
  - **Features**: Cloud-based security and compliance solutions.
  - **Benefits**: Provides vulnerability management, compliance monitoring, and risk assessment.

1. Policy and Compliance Management

- ** **Qualys Cloud Platform**: Offers robust solutions for vulnerability management, policy compliance, and security configuration assessments. Ideal for comprehensive compliance management and risk assessment.
- ** **OneTrust**: Known for its extensive compliance management features, including GDPR and CCPA compliance, privacy impact assessments, andpolicy management.

2. Data Inventory and Classification

- ** **Varonis Data Security Platform**: Provides advanced data discovery, classification, and protection, helping to identify and secure sensitive data across various platforms.
- ** **Collibra**: Excellent for data governance and management, including data cataloging, inventory, and classification, with strong integration capabilities.

3. Data Access and Encryption

- ** **Microsoft Azure Active Directory**: A comprehensive identity and access management solution that integrates well with Microsoft ecosystems and provides strong access control features.
- ****Symantec Data Loss Prevention (DLP)**: Offers extensive data encryption and protection solutions, both at rest and in transit, with robust policy enforcement.

4. Data Retention and Disposal

- ** **Netwrix Auditor**: Provides effective monitoring and auditing of data changes, helping to enforce data retention policies and ensure compliance.
- ** **Blancco Data Eraser**: A leading solution for secure data erasure, ensuring that data is effectively destroyed according to industry standards.

5. Encryption on Devices and Remote Wipe

- ****BitLocker (Microsoft)**: A reliable solution for full-disk encryption on Windows devices, providing strong protection for data at rest.
- ** **Microsoft Intune**: Offers comprehensive mobile device management, including remote wipe capabilities, which is ideal for managing and securingportable devices.

6. Data Management Controls

- ** **IBM Guardium**: Excellent for monitoring and safeguarding data in both physical and digital forms, with features for data activity monitoring and security controls.
- ** **SecureWorks**: Provides managed security services and robust data protection for both physical and digital data.

7. Data Analytics Compliance

- ** **Talend Data Fabric**: A versatile platform for data integration, quality, and governance, with features that support compliance with various regulations.
- ** **SAS Compliance Solutions**: Ideal for data analytics that need to adhere to complex regulatory requirements, offering tools for compliance management and reporting.

8. Oversight and Metrics Review

- ** **Tableau**: Provides powerful data visualization and reporting tools, ideal for creating dashboards and metrics that support oversight and performance tracking.
- ** **Splunk**: Offers robust operational intelligence and analytics capabilities, allowing for real-time monitoring and metric tracking for security and compliance.

9. General Auditing and Validation Tools

- ** **AuditBoard**: Streamlines audit processes with features for planning, execution, and reporting, making it easier to manage audits and track compliance.
- ** **Nessus**: A leading vulnerability assessment tool that helps identify and address security weaknesses across your environment.

10. Additional Considerations

- ** **Tenable.io**: Provides a cloud-based vulnerability management platform that offers comprehensive visibility and continuous monitoring of your IT environment
- ** **Splunk Enterprise Security**: Offers a broad range of security information and event management (SIEM) capabilities, useful for comprehensive monitoring and incident response.

Recommendations Based on Use Case

- **For Small to Medium Enterprises (SMEs): BitLocker** for encryption, **Netwrix Auditor** for data retention and auditing, and **Collibra** for data governance are good choices due to their scalability and comprehensive features.
- **For Large Enterprises: IBM Guardium** and **Qualys Cloud Platform** offer robust solutions for complex environments with extensive compliance and security needs.

Notes

Monday, September 16, 2024 4:41 PM

The
ISA learned in an interview with organizational staff that the organization is working to implement a data classification policy by September 2024.

Questions

Monday, October 28, 2024 8:04 AM

Data Management Controls

Policy or Program for Data Management

1. **Is there a formal policy or program in place for data management?**
2. **Does the policy define roles and responsibilities for data management?**
3. **Is this policy reviewed and updated regularly to reflect regulatory and operational changes?**

Data Inventory Established

1. **Has the credit union established a comprehensive inventory of data assets?**
2. **Does the data inventory categorize data types based on sensitivity, owner, and storage location?**
3. **Is the data inventory reviewed and updated periodically to capture new data assets?**

Data Access List Established

1. **Is there a documented list of individuals who have access to sensitive data?**
2. **Are access privileges assigned based on roles and the principle of least privilege?**
3. **Are access lists reviewed regularly to ensure only authorized personnel have access?**

Data Retention Enforced

1. **Is there a defined data retention policy aligned with regulatory and business requirements?**
2. **Are data retention schedules consistently enforced across all systems?**
3. **Is there a process to ensure data is removed or archived per retention policies?**

Data Disposal Based on Sensitivity

1. **Are there procedures for securely disposing of data based on its sensitivity?**
2. **Is data destruction documented and validated to ensure compliance with disposal policies?**
3. **Are personnel trained on the procedures for secure data disposal?**

Encryption on End-User Devices

1. **Is sensitive member data encrypted on all end-user devices (e.g., laptops, mobile devices)?**
2. **Are there controls to ensure encryption policies are consistently applied on end-user devices?**
3. **Is compliance with encryption requirements monitored regularly?**

Encryption of Sensitive Data at Rest and in Transit

1. **Is sensitive data encrypted both at rest and during transmission?**
2. **Are encryption standards for data at rest and in transit aligned with industry best practices?**
3. **Is encryption reviewed periodically to ensure it remains effective and current?**

Remote Wipe Process for Portable Devices

1. **Is there a remote wipe capability for company-owned portable devices containing sensitive data?**
2. **Are procedures established to initiate remote wipe in the event of device loss or theft?**
3. **Are remote wipe processes periodically tested to ensure functionality?**

Safeguarding Data in Physical and Digital Form

1. **Are physical and digital safeguards in place to protect sensitive data?**
2. **Are there procedures to regularly assess the effectiveness of these safeguards?**
3. **How are potential gaps or vulnerabilities in safeguarding identified and addressed?**

Documenting Data Types, Owners, Users, and Purpose

1. **Is there documentation specifying the types of data maintained, including data owners, users, and its purpose?**
2. **Are data owners and custodians responsible for regularly updating this documentation?**
3. **Is this information used to facilitate reporting and decision-making processes?**

Controlling Non-Masked Data in Non-Production Environments

1. **Are processes in place to control the use of non-masked data in non-production environments?**
2. **Is there monitoring to ensure non-production environments do not expose sensitive data?**
3. **Is data masking consistently applied when using real data for testing or development?**

Removal or Destruction of Data in Analytics Tools

1. **Are procedures established to remove or destroy data from analytics tools when it is no longer used?**
2. **Is there documentation of data removal processes to support compliance with this requirement?**
3. **How often is the data removal or destruction process audited?**

Compliance of Data Analytics Processes with Regulations

1. **Are data analytics processes reviewed to ensure compliance with applicable laws and regulations, such as the Bank Secrecy Act?**
2. **Are data analytics activities documented to demonstrate compliance efforts?**
3. **How does management ensure ongoing alignment of data analytics processes with regulatory requirements?**

Oversight Committee with Board and Management Representation

1. **Is there an established oversight committee with board and management representation for data management?**
2. **Does the committee have documented responsibilities for overseeing data management practices?**
3. **How often does the committee meet to discuss data management-related issues?**

Regular Review of Information Security Program Metrics

1. **Does the oversight committee regularly review metrics demonstrating the effectiveness of the information security program?**
2. **What types of metrics are reviewed to assess compliance with data management policies?**
3. **Are corrective actions taken if metrics indicate deficiencies in the information security program?**

Answers

Monday, October 28, 2024 8:04 AM

Stmt 19: Data Management Controls

Stmt 19.1: Policy or Program for Data Management

1. **Positive**: "Yes, a formal data management policy is documented, updated annually, and includes defined roles and responsibilities."
    - **Negative**: "No formal policy exists, or it lacks clear responsibilities and a regular review cycle."
2. **Positive**: "The policy clearly assigns data stewardship roles and responsibilities across departments."
    - **Negative**: "Roles are not defined, or there is inconsistency in role assignment and adherence."
3. **Positive**: "The data management policy is reviewed annually and updated with regulatory or operational changes."
    - **Negative**: "The policy has not been reviewed in over a year or lacks any recent updates to meet current requirements."

Stmt 19.2: Data Inventory Established

1. **Positive**: "Yes, a complete and regularly updated inventory of data assets is maintained."
    - **Negative**: "A data inventory is not established or is outdated and lacks comprehensiveness."
2. **Positive**: "Data assets are classified by sensitivity, owner, and location, with up-to-date categorization."
    - **Negative**: "Data categorization by sensitivity, owner, and location is either absent or incomplete."
3. **Positive**: "The inventory is reviewed quarterly and includes new data assets."
    - **Negative**: "No review process exists, or reviews are infrequent and fail to account for new assets."

Stmt 19.3: Data Access List Established

1. **Positive**: "Data access is documented, ensuring access lists are up-to-date and aligned with roles."
    - **Negative**: "No access list exists, or it is outdated, with several unauthorized personnel having access."
2. **Positive**: "Access is role-based, ensuring compliance with the principle of least privilege."
    - **Negative**: "Access is granted beyond role requirements, violating the principle of least privilege."
3. **Positive**: "Access lists are reviewed monthly to ensure only necessary access is maintained."

  - **Negative**: "Access lists are rarely reviewed, resulting in outdated permissions and potential security risks."

Stmt 19.4: Data Retention Enforced

1. **Positive**: "Retention policies are established and followed, with automated deletion after the retention period."
    - **Negative**: "No retention policy is enforced, resulting in data being retained longer than necessary."
2. **Positive**: "Retention schedules are systematically implemented across all data repositories."
    - **Negative**: "Retention schedules are inconsistently applied, leading to gaps in enforcement."
3. **Positive**: "Regular audits confirm data is deleted or archived as per retention schedules."
    - **Negative**: "No audit process is in place, and excess data may remain in systems indefinitely."

Stmt 19.5: Data Disposal Based on Sensitivity

1. **Positive**: "Procedures exist to securely dispose of data based on sensitivity, with proper documentation."
    - **Negative**: "Data disposal lacks clear procedures, risking unauthorized data exposure."
2. **Positive**: "Destruction methods are aligned with data sensitivity and are properly documented."
    - **Negative**: "Destruction methods are inconsistent or undocumented, leading to potential data leaks."
3. **Positive**: "Employees receive training on secure data disposal procedures annually."
    - **Negative**: "No training is provided on disposal practices, increasing risk of improper disposal."

Stmt 19.6: Encryption on End-User Devices

1. **Positive**: "End-user devices are fully encrypted to protect member data, with ongoing monitoring."
    - **Negative**: "Not all end-user devices have encryption enabled, risking unauthorized access to data."
2. **Positive**: "Policies ensure consistent encryption on devices handling sensitive data."
    - **Negative**: "Encryption policies are not enforced or consistently applied."
3. **Positive**: "Compliance with encryption policies is reviewed monthly."
    - **Negative**: "No compliance review exists, and data is potentially unprotected on devices."

Stmt 19.7: Encryption of Sensitive Data at Rest and in Transit

1. **Positive**: "Sensitive data is encrypted at all times, whether in storage or during transmission."
    - **Negative**: "Sensitive data is only partially encrypted, exposing it to potential

threats."

2. **Positive**: "Encryption standards meet industry best practices and are regularly updated."
    - **Negative**: "Encryption standards are outdated and not reviewed periodically."
3. **Positive**: "Quarterly encryption audits confirm compliance with encryption requirements."
    - **Negative**: "No audits are conducted, leading to unknown encryption coverage."

Stmt 19.8: Remote Wipe Process for Portable Devices

1. **Positive**: "All portable devices have remote wipe functionality, which is tested regularly."
    - **Negative**: "Remote wipe capability is not universally enabled on portable devices."
2. **Positive**: "Clear protocols are in place for initiating remote wipe in case of device loss or theft."
    - **Negative**: "Remote wipe procedures are inconsistent or undocumented, leading to potential data exposure."
3. **Positive**: "Periodic tests confirm that remote wipe functions as expected."
    - **Negative**: "No tests are conducted, so remote wipe functionality may be unreliable."

Stmt 19.9: Safeguarding Data in Physical and Digital Form

1. **Positive**: "Data safeguards meet regulatory and organizational standards for security."
    - **Negative**: "Safeguarding measures are incomplete, leaving data at risk."
2. **Positive**: "Regular assessments are conducted to evaluate safeguard effectiveness."
    - **Negative**: "Safeguards are not assessed, resulting in unidentified vulnerabilities."
3. **Positive**: "Identified vulnerabilities are promptly addressed and documented."
    - **Negative**: "Vulnerabilities remain unaddressed due to lack of monitoring."

Stmt 19.10: Documenting Data Types, Owners, Users, and Purpose

1. **Positive**: "Data types, ownership, and purposes are documented to support transparency and accountability."
    - **Negative**: "Documentation of data attributes is incomplete, lacking essential details."
2. **Positive**: "Documentation is regularly updated to capture new data assets and ownership changes."
    - **Negative**: "No updates are made to reflect new data or ownership changes."
3. **Positive**: "Documentation is used for reporting and supporting decision-making processes."
    - **Negative**: "Documentation is inaccessible or outdated, limiting its use in reporting."

Stmt 19.11: Controlling Non-Masked Data in Non-Production Environments

1. **Positive**: "Non-production environments are configured to prevent exposure of non-

masked data."

  - **Negative**: "Non-masked data is accessible in non-production environments, risking data exposure."

2. **Positive**: "Monitoring tools are in place to detect and prevent unauthorized data use."
   - **Negative**: "No monitoring exists, so non-masked data could be inadvertently exposed."
3. **Positive**: "Data masking is strictly enforced for testing and development purposes."
   - **Negative**: "Data masking is inconsistent or ignored, risking data privacy."

Stmt 19.12: Removal or Destruction of Data in Analytics Tools

1. **Positive**: "Data is removed from analytics tools when no longer in use, following documented procedures."
   - **Negative**: "Data remains in analytics tools indefinitely, increasing retention risks."
2. **Positive**: "All data removal or destruction is logged for compliance."
   - **Negative**: "No documentation exists for data removal, creating potential compliance gaps."
3. **Positive**: "Data removal is audited quarterly to verify adherence to policies."
   - **Negative**: "No audits occur, so data removal may be inconsistently applied."

Stmt 19.13: Compliance of Data Analytics Processes with Regulations

1. **Positive**: "Data analytics processes are compliant with all applicable regulations."
   - **Negative**: "Data analytics processes do not account for regulatory requirements, risking non-compliance."
2. **Positive**: "Processes are reviewed and adjusted as regulations evolve."
   - **Negative**: "Reviews are infrequent, leading to potential regulatory exposure."
3. **Positive**: "Documentation demonstrates that analytics processes meet regulatory expectations."
   - **Negative**: "Documentation is insufficient to support regulatory compliance."

Stmt 19.14: Oversight Committee with Board and Management Representation

1. **Positive**: "The oversight committee includes board and management representatives with defined responsibilities."
   - **Negative**: "The committee lacks board or management representation, limiting oversight effectiveness."
2. **Positive**: "The committee meets regularly and documents its findings and decisions."
   - **Negative**: "Meetings are infrequent, and decisions are not documented."
3. **Positive**: "The committee proactively reviews data management issues and updates policies as needed."
   - **Negative**: "The committee is not engaged with current data management practices."

Stmt 19.15: Regular Review of Information Security Program Metrics

1. **Positive**: "Metrics are reviewed regularly to assess the program's effectiveness, with actions taken for any deficiencies."
    - **Negative**: "No metric review process exists, so the program’s effectiveness remains unassessed."
2. **Positive**: "Key metrics are tracked, and findings are communicated to management."
    - **Negative**: "Key metrics are not tracked or reported, reducing program transparency."
3. **Positive**: "The program is adjusted based on metric reviews to improve outcomes."
    - **Negative**: "Program adjustments are infrequent, leading to ongoing vulnerabilities."