Privacy Technical Assistance Center

For more information please visit the Privacy Technical Assistance Center: http://nces.ed.gov/ptac

Responding to IT Security Audits: Improving Data Security Practices

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on http://nces.ed.gov/programs/ptac.

Purpose

Information Technology (IT) audits can help organizations identify critical gaps in data security and reduce the threat of security compromises. This issue brief explains what audits are and how they can be used to improve data security. It also provides recommended steps for developing an effective audit response plan, which is a detailed, point-by-point plan for addressing security concerns uncovered by an audit. Recommendations relate to collaborating with auditors to confirm understanding of an audit report, prioritizing audit findings, and determining corrective actions and implementation schedules. The recommendations included in this brief are intended to help educational organizations maximize the value of IT audits and improve data security. Examples of appropriate responses to audit findings are included in the appendix.

What is an IT security audit and how can it benefit an education organization?

An IT security audit is an assessment of an information system's security architecture and processes, as well as all related policies and procedures for managing data in a secure manner. Audits are usually performed by trained staff in an organization, partners in state or federal government agencies, or third party experts in data security. The frequency with which audits occur depends on the sensitivity of the information stored in the data system, resources available to the organization, and the priority given by the organization to the audit process.

At the state level, auditors are often independent experts responsible for ensuring that educational data systems meet industry or government standards for data protection. When auditors are not available at the state level, educational organizations should develop their own audit capabilities or hire third-party experts to assess the security of their information system.

Security audits can help organizations identify critical gaps in data security, and subsequently decrease the likelihood of a security compromise. Working closely with auditors *before*, *during*, and *after* an audit allows an organization to better understand the strengths and weaknesses of its security technology, policies, and procedures. Working with experienced auditors also allows organizations to learn about best practices in data security.

While audits are a powerful IT security tool, they are *only one* aspect of a comprehensive data security program, which also should include:

- physical security;
- security architecture (e.g., connection management, encryption, etc.);
- identity management and access control;
- threat assessment and vulnerability management (including configuration control and audits);
- security operations (e.g., monitoring, detection, and incident management); and
- continuity of operations and disaster recovery planning.

See glossary for definitions of these terms.

The Audit Process

Although customized to meet an organization's specific technology, data, and security needs and circumstances, audits generally follow a customary set of steps designed to familiarize auditors with the organization's IT system and potential areas of concern. Many auditors rely on the following general protocol to conduct a comprehensive IT audit:

1. Meet with the organization's officials and key personnel to develop or confirm understanding of the organization's data, information needs, systems architecture, system use, and unique security requirements.
2. Establish objectives for the audit. For example, determining what systems will be audited, what security activities will be reviewed, what privacy regulations will be evaluated, etc.
3. Review IT security policies and processes, with an emphasis on data center procedures and security capabilities.
4. Perform the security review, often focusing on network vulnerabilities, security controls, encryption, access control and user accounts, password management, etc.
5. Issue a report with detailed findings.

Audit Response Recommendations

Organizations should respond to IT security audit findings by developing a detailed, point-by-point plan for addressing security concerns uncovered by the audit. This audit response plan should include specific solutions for each identified weakness and an implementation timeline for each solution. A sound audit response plan also specifies who is responsible for each task, how each capability area will be managed, expectations for senior management involvement, the ramifications of proposed solutions on current business practices, and how potential conflicts between business practices and security needs will be resolved.

While the audit response plan will guide the implementation of corrective actions for the audited organization, it is also a useful tool for the auditing agency, as it provides auditors with confidence that the audited organization is assigning the appropriate resources necessary to resolve issues identified in the audit. The following steps will help an organization develop an effective audit response plan:

1) *Meet with Auditors* – Before developing an audit response plan, an organization must first fully understand its audit findings, which can be complex and highly technical in nature. Staff members responsible for developing the audit response plan should meet with auditors to review all findings, correct any mistakes, and clarify questions or concerns about the findings. The following actions can help make a meeting with auditors especially productive:

   - ✓ Meet with the personnel who actually performed the audit and wrote the findings.
   - ✓ Discuss each finding to clarify what was found. This is an opportunity to correct any misinformation or misunderstanding by the auditors. If any errors were found in the auditor's analysis, request a re-issue of the final report to reflect corrections.
   - ✓ Ask for the auditor's advice on ways to correct the problems. What have they seen as viable solutions in comparable organizations?
   - ✓ Ask whether auditors are available to review a draft of the audit response plan prior to implementation.
   - ✓ Schedule a follow-up meeting when the proposed responses have been completed in order to verify that sufficient corrective steps have been taken to address each audit finding.

2) *Prioritize Tasks* – If time or resources prevent the immediate implementation of corrective actions for *all* audit findings, the audit response plan must identify which findings are the most critical, plan corrective actions to address these findings first, and accept that lower priority concerns must be dealt with at a later time (which should still be scheduled in the plan).

   Security audit reports often rank security deficiencies and prioritize remediation tasks for the client. Tasks are frequently identified as high, medium, or low priority, or ordered by another ranking convention. Alternatively, findings may be presented to an organization without having been assigned priority. In either case, the organization needs to prioritize response activities, which must be evaluated from the perspectives of criticality for IT security, cost, and the availability of human resources to implement a response. In some cases, it may be useful to have an independent third-party expert review and assess the findings and assist with prioritizing responses. It is important to consider a wide range of factors when prioritizing audit responses, including:

   - ✓ input from the report and meeting with auditors;
   - ✓ cost, including consideration of whether, for example, implementing one high priority finding is a better option than addressing four medium priority findings;
   - ✓ staffing capabilities, including whether the organization has the appropriate personnel to implement the finding or if outside assistance is required;
   - ✓ nature of solutions, including consideration of which findings can be resolved with policy changes and which require technical solutions;
   - ✓ contractual concerns, such as whether contracted support is required and, if so, the time necessary to get contracts in place;
   - ✓ management support, such as what level of organizational approval is necessary to implement solutions; and
   - ✓ scope issues, such as whether a finding can be implemented solely on the authority of the IT department or whether further coordination is required.

3) *Identify Corrective Actions* – IT security audit findings often require the introduction of new technical solutions or more effective deployment of existing solutions in or outside IT. For example, if an audit report finds that a particular social media site has repeatedly infected the network, this may require a technical intervention to block the site. Occasionally, non-technical solutions, such as policy and procedural changes, can address vulnerabilities. In the case of a troublesome website, if the organization cannot control access to the site through a technical intervention, a written policy that forbids access can be an effective alternative. It is important, however, to consider any unintended impacts corrective actions may introduce across the organization. After all, a new policy that bars access to a social media site may have an adverse impact on the Human Resources (HR) department, which may use the site for recruiting purposes. In such an instance, an exception to the policy *may* be warranted to permit HR personnel to access the site, or it may be necessary to segment their operations from the network.

   Depending on expertise available from within the organization, corrective actions may be identified by staff, auditors, or contracted third-party experts. Answers to the following questions will help planners identify and select appropriate corrective actions:

   - ✓ If a preferred solution is cost-prohibitive, is a less expensive alternative viable?
   - ✓ Is the solution “plug and play” or does it require customization, monitoring, and ongoing fine tuning? Who will maintain it?
   - ✓ Are there solutions that address more than one audit finding?
   - ✓ Is a solution available for a trial period to ensure that it is compatible with the organization’s other technologies and that it performs to expectations?
   - ✓ Is a technical solution required or can physical security, access control procedures, or new policies remedy the finding?
   - ✓ Are these long-term or short-term solutions?

4) *Develop an Implementation Schedule* – The primary purpose for developing an audit response plan is to ensure the effective remediation of security concerns *in a timely manner*. While efforts to plan, allocate resources, and implement solutions take time, delays in addressing security concerns make organizations more vulnerable to threats. When developing a schedule, the organization should make an effort to:

   - ✓ be realistic about the time needed to develop and implement proposed solutions, accepting that the “real world” often introduces unplanned obstacles to tasks and delays to implementation schedules;
   - ✓ balance the time required to implement “ideal” solutions against risks associated with prolonged exposure while awaiting development and implementation;
   - ✓ investigate the costs and benefits of temporary solutions that, by definition, may not be permanent, but can improve security relatively quickly while longer term solutions are developed;
   - ✓ meet any correction deadlines imposed by the auditing agency (if the auditor has such authority); and
   - ✓ develop intermediate milestones, phased-in implementation targets, and internal sub-task level completion dates in addition to the timeline for completing the entire audit response plan.

5) *Confirm Plans with Senior Management and Regulatory Authorities* – Because data security is a high-profile concern, especially when evaluated in light of the types of personally identifiable information (PII) maintained by education organizations, the organization should make every effort to ensure that senior management approves and supports the audit response plan. Tips for doing so include:

   - ✓ sharing a draft of the plan with senior management and external authorities as appropriate—being sure to note the confidential nature of the audit response plan, which, by definition, documents current weaknesses and planned security strategies;
   - ✓ offering to explain the plan and answer questions that arise;
   - ✓ confirming approval of the human and financial resources necessary to ensure successful implementation and ongoing maintenance of the comprehensive security plan; and
   - ✓ requesting formal approval and support for the audit response plan.

6) *Deliver on the Plan* – Auditors, senior management, external authorities, and others involved in the audit process will expect that all serious security deficiencies identified in an audit be remedied in a timely manner. Do so and provide auditors with feedback on the implementation of corrective actions.

7) *Prepare for Future Audits* – Previous audit findings and promised corrective actions will often be a focus of future audits. Establishing an ongoing dialogue with auditors will eliminate many surprises during subsequent audits.

Please note that all recommendations included in this issue brief are intended to complement, not supersede, an organization's local security regulations and policies.

APPENDIX: Examples of audit response plans with appropriate specificity

Example 1. Audit Finding: No clear management plan to implement correct security measures.

Response: The Chief Information Security Officer (CISO) is managing the corrective actions required to address these capabilities areas. Program managers have been assigned to lead and implement each of the capabilities outlined below. They are responsible for monitoring progress and will report project status on a weekly basis to the CISO. Monthly status updates will be provided to senior management. Any potential delays to the implementation schedules will be addressed by one of the following methods:

Specificity of Management Responsibility →

- Technology: A team will be established to review the problem and evaluate and test potential corrective actions or identify an alternative method to achieve the desired end-state.
- Production: Program managers and the CISO will review the problem and adjust schedules so as not to delay production.
- Contractual: The contracts office will work with all contractors to resolve issues and secure additional resources as required.

Example 2. Audit Finding: Two-factor authentication for internal users not fully implemented.

Response: The goal of the rollout is that all employees and contractors will use two-factor authentication for their government-issued desktops and laptops to access the enterprise network by the end of Fiscal Year 2011 (FY11). The implementation schedule for two-factor authentication will be as follows:

1) Identification of preferred solution and integration with IT (complete)
2) Training and awareness (Jan-June FY11)
3) Certification and accreditation (March FY11)
4) Operational testing and evaluation (July FY11)
5) Implementation

Specificity of Action Items →

a. 20 percent of users transitioned no later than June 1, 2011
b. 60 percent of users transitioned no later than July 1, 2011
c. 100 percent of users transitioned no later than September 1, 2011

Glossary

Access control is a system that enables an authority to control access to areas and resources in a given facility or computer-based information system.

Computer security operations is a term used to describe the active component of information security that includes network monitoring, intrusion detection, configuration management, access control, and incident management.

Configuration management, also referred to as Secure Configuration Management , can be defined as the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, and test documentation throughout the life cycle of an information system.

Connection management is the process of identifying, introducing, controlling, monitoring, and removing a transmission path between two or more points.

Disaster recovery encompasses the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning to keep critical aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the technology systems that support business functions.

Encryption is the process of transforming information using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key.

Identity management (ID management or IdM) is a broad administrative area that deals with identifying individuals in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity.

Physical security describes measures that are designed to deny physical access to unauthorized personnel (including computer hackers) to a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts.

Personally identifiable information (PII) refers to information, such student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR §99.3, for a complete definition of PII specific to education data and for examples of education data elements that can be considered PII.

Security architecture is a subset of the IT architecture pertaining to the network design details and controls (countermeasures) that protect the enterprise from computer threats. The purpose of the security architecture is to establish and maintain the information security posture of the network and provide confidentiality, integrity, and availability.

Threat assessment is a formal evaluation and description of the threats to an information system.

Vulnerability management is an IT security program or process that describes the current security posture, prioritizes vulnerabilities, mitigates those vulnerabilities, and maintains and monitors those mitigations.