How to Protect Your District from the Three Most Common IT Audit Findings

by Emily A. Powell, CPA, Staff Associate II

Posted on October 22, 2020

We have entered 2020, a new decade which seems to revolve around information technology (IT). As with the rest of the working world, audit requirements and test work over IT are growing at a rapid pace. The IT portion of the annual audit is expanding due to districts hosting and processing more financial and student data electronically than ever, which greatly increases the risk of external and internal threats. In addition, the Auditor General frequently adds new compliance questions to the Uniform System of Financial Records (USFR). Due to the State's increasing interest in information technology, all districts should expect a more in-depth review of their IT function when their annual audit rolls around.

However, new requirements can sometimes lead to unforeseen audit findings. Below are three of the most common IT audit findings, with resources and/or solutions for each. Following these recommendations and checks of controls will better help you prepare for the ever-growing IT portion of your audit. In addition, it will help increase your protection of student data, financial records, etc.

Board Adopted Policies

The first common IT finding is a lack of robust Board-adopted IT policies. Districts should routinely be updating their IT policies to match all of their current procedures, controls, risk management analyses, etc. Below are four resources to help strengthen your current IT policies.

- The first place you can look for some guidance is the USFR for Arizona School Districts. The section pertaining to Information Technology starts on page 227 of the PDF. This can help guide the topics that should be covered in your IT policies, as well as give ideas of general IT controls to implement. Along with this, it is important to stay current on the USFR Compliance Questionnaire IT questions, particularly, questions 2-5 in the IT subsection relate to policies. To ensure compliance with these questions, districts should verify that the following four items are referenced in their policies.
    - Explaining who is responsible for and the process behind IT configuration changes (including programming, operating, and modifying of the system(s)).
    - Discussing security risks of unauthorized access to district systems, network, and data including e-mail, internet use, VPN, wireless access and mobile devices.
    - Documenting any procedures in place for employee awareness training over prevention and detection of technology-related threats. This includes guidelines on the response to specific incidents. This could potentially involve employees signing an acceptance of IT training documents upon hire or annually.
    - Recording the process of immediately removing or modifying terminated or transferred employees and/or vendors access to district systems.
- Next, the Government Accountability Office (GAO) periodically releases their "green book". This is a good resource for all controls, but the design of IT controls starts on page 53. This document can also provide a basis for what controls to document and common control language to include in your policies.
- Utilize the Arizona School Boards Association (ASBA) Policy Bridge for examples and templates of IT policies adopted by other districts.
- Finally, if applicable, consult with your third party IT vendor to help draft updated policies. They may be better able to explain the various IT controls your systems and applications already have in place. For example, they might be more familiar with the anti-virus, anti-malware, or system patches that are being utilized.

General External Security Controls

In this day and age, IT and security breaches seem to go hand in hand. That is why it is so important for districts to implement control procedures that restrict unauthorized users from gaining access to district systems and databases. Below are four control recommendations that reduce the risk of external security threats.

- Require complex passwords with at least eight characters for all district computers.
- Implement screen locks on all district computers.
    - General recommendation: A 10-minute idle period before the computer locks out.
- Program all district computers to disable access for a certain period of time if it experiences repeated failed sign in attempts.
    - General recommendation: A 30-minute lockout after five failed log in attempts. In addition, failed log in attempts can trigger an automatic email be sent to the IT department as an additional control.
- Adopt a policy prohibiting the sharing of user IDs and passwords. This could also include employees signing an "IT user agreement" upon hire or annually.

Internal Controls – Limiting Employee Access

While external IT threats are often thought of first, it is just as imperative for districts to analyze the risk of internal threats. All districts should be implementing employee access controls over all systems to minimize the risk of override, superfluous access, and weakened segregation of duties. Below are four recommendations on how to avoid unnecessary employee accesses:

- Conduct an annual internal audit of each employee's system access. Evaluate if access levels are reasonable and necessary based on job duties. This could entail employees making a list of their day-to-day job duties and identifying which modules they need full access, read-only access, or no access. Turn off all unnecessary accesses/modules.
- When faced with turnover, do not immediately grant the replacement employee the same access as the former employee. Take the time to analyze the job duties of the replacement position and build an access profile around these functions. It is safer to begin with limited access levels and subsequently turn on needed modules rather than starting with full access and retroactively turning off unnecessary modules.
- Contact your IT system provider regarding the creation of temporary access. This could be useful during times of high turnover, when it is sometimes necessary for employees to perform abnormal job duties until a new staff is hired. This, however, should trigger additional review procedures for employees serving as the "back-up" role. This could include reviewing change logs, requiring two approval signatures, or conducting a physical review.
- Ask your provider if your IT system(s) can generate a report showing each time user accesses are modified and implement a review process over this report to ensure the oversight of appropriate employee accesses year round.

Although the above information is not a comprehensive list of all IT areas and controls that might be tested in an audit, it does provide a starting point of what controls and processes to improve upon. The IT area, along with how to test it, will continue to adapt and grow the more reliant districts become on electronic processing. Make sure your district is staying ahead of the curve, routinely updating policies when necessary, and actively reducing the risk of external and internal threats through strengthened controls.