IT Audits: What, Why, Who, and When

By Allison Davis, Senior Manager and Katie Kane, Manager

IT audits. Those two little words make many people feel anxious, but they shouldn't. The purpose of IT audits isn't to get you or your IT team in trouble. It's to help your organization assess your existing information technology (IT) controls and address any areas where controls can be added or improved. The end goal is to make your organization more secure.

Let's explore the what, why, who, and when of IT audits so you understand the important role they can play at organizations of all sizes.

What IT Audits Are

An IT audit is the process of examining and evaluating the risks and mitigating controls surrounding an organization's IT environment. The scope can vary based upon an organization's need, ranging from a more limited review of controls surrounding a specific asset or function to a broader review encompassing the control framework of a department or the entire organization.

Regardless of the scope, IT audits often include a review of physical, technical, logical, and operational security controls and consider compliance with critical aspects of corporate governance and applicable laws and regulations.

Why Your Organization Should Consider an IT Audit

An organization may want to have an IT audit performed to:

- **Provide checks and balances for the IT department**. Various aspects of your organization are probably audited already. Your accounting department's practices are reviewed as part of a financial statement audit. If you are a higher education institution that provides financial aid, you likely have a periodic student financial aid audit.

  The IT department should be treated no differently. It's not that you don't trust your IT staff. Instead, you understand that life happens. Challenges such as staff turnover, functions shifting or being overlooked, inadequate communication, and an overworked and understaffed department can lead to issues. IT audits can pinpoint these deficiencies and identify areas that need resolution.
- **Gain support for additional security resources.** Budget and staffing limitations are two of the biggest obstacles to security. Because IT departments typically don't produce income, it often becomes difficult to justify staffing or technology expenditures to help make the department more secure, efficient, and effective. When an independent party makes recommendations for improvements, it can often hold more weight than if the IT staff made the request themselves. Management is often more likely to provide the funds and support needed as a result of audit deficiencies.
- **Provide the opportunity to fix deficiencies before they become a true problem.** Many organizations handle sensitive information about donors, employees, students, and other constituents. Privacy laws and regulations related to protecting this information are becoming more commonplace, and noncompliance could result in significant financial and reputational impact through loss of trust, fines, penalties, notification requirements, and legal fees. IT audits can help you identify and resolve control weaknesses that could increase the risk of unauthorized access to and compromise of this sensitive information.
- **Keep pace with an ever-changing threat landscape.** IT risks are constantly evolving, and the controls to mitigate these risks cannot be stagnant. An effective IT audit is a vital tool to help your IT environment keep pace with the ever-changing threat landscape.

Who Performs IT Audits

IT audits can be performed by staff members or a third party. Whether the audit is internal or external, however, the auditor should be independent of the area being audited. For example, just as you wouldn't want your CFO auditing your financial statements, you don't want your IT

manager auditing the controls he or she has implemented. The IT manager is likely responsible for daily compliance with those policies, procedures, and controls, but the audit should be independent to provide a point-in-time check for the IT department.

When IT Audits Should Be Performed

Controls should be tested at least annually, and you may decide that higher-risk areas need more frequent testing. And if you have internal IT audits, it's a best practice to have an external audit periodically to provide a fully independent check. While your internal IT audit team may be independent of the IT department, internal IT audits typically are more subjective and can omit control areas or recommendations for various reasons.

Many organizations contract an external firm to perform an IT audit every 12 to 24 months and conduct internal audits in the interim periods.

Now that you understand what IT auditing is and why it's important, it's time to get auditing! Check out How to Develop an Effective IT Audit Program for steps to help your organization develop an effective IT audit program.

About the Authors

Allison Davis, Senior Manager
CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

Katie Kane, Manager
CapinTech
kkane@capincrouse.com
o 505.50.CAPIN ext. 2007

Katie has 15 years of banking technology experience and nearly four years of information security auditing experience. Katie also has an extensive knowledge of Automated Clearing House (ACH) rules and regulations and is the ACH specialist on staff. She stays current on changing threats and government regulations to better assist clients in protection against cybersecurity threats.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.