How to Develop an Effective IT Audit Program

By Allison Davis, Senior Manager and Katie Kane, Manager

An IT audit helps organizations of all sizes assess their information technology (IT) controls and pinpoint and address deficiencies. In other words, it's an important cybersecurity tool.

This article provides an overview of IT audits and explores why your organization should consider them. Now we'll look at how to develop an IT audit program at your organization.

Whether you choose to perform your audits with an internal team or contract with an external firm, the four steps below will help ensure that your IT audit program is efficient and effective.

Step 1: Assess risks.

All audits should be based on a risk assessment, a process to identify the areas that should be given the highest priority. This helps you avoid devoting time and resources to auditing areas with low risk or low impact for your organization.

Start by identifying all your technology, assets, and data and the threats associated with each. Then document the controls that mitigate each risk to depict how those risks are reduced to an acceptable level.

Some areas, such as network security, are inherently high-risk and should be audited annually. But the risk assessment can guide you in determining what other areas should be included in your IT audit.

Keep in mind that something that poses a low risk to your organization one year may be sufficiently high-risk in the next. Your IT audit plan should constantly evolve with your risk assessment.

Step 2: Design the IT audit.

Before beginning an audit, it's imperative to formally define the scope to ensure all involved parties are aware of what will be included. This will give you a framework and keep resources focused on the key areas that need to be reviewed.

Consider the following:

- Are you evaluating a specific application, department, function, or service line?
- Will the audit be a more encompassing review of general controls?
- Are you reviewing overall security to make recommendations for control enhancement?
- Are you testing compliance with defined policies and procedures?

Once you've identified the scope, the next step is to design the audit procedures necessary to meet the goals of the audit. If the IT audit is being performed by internal staff, they will typically design the audit procedures. If the audit is performed by an external party, you generally will have less involvement in developing the audit procedures and the external party will use their professional judgment to meet the objectives of the audit.

Step 3: Begin the IT audit.

After you've defined the scope and the IT audit procedures have been developed, it's time to begin gathering information relevant to the areas being audited. This can range from confirmation of application security controls to patch and anti-malware management reports and documented policies and procedures. Supporting documentation is important to provide evidence and confirmation that policies and procedures are being

Something that poses a low risk to your organization one year may be sufficiently high-risk in the next. Your IT audit plan should constantly evolve with your risk assessment.

adhered to. It can also provide insight into exceptions or processes that are not functioning as intended.

Once the information-gathering phase is complete, the auditor should review the audit documentation and schedule interviews with appropriate staff members. This should help the auditor:

- Determine whether policies and procedures are being adhered to
- Identify whether existing controls are sufficient to mitigate applicable risks
- Uncover areas of concern

Any supporting information from interviews or documentation review should be detailed in audit notes. This will help the team answer questions or support recommendations in discussions with management and the IT staff. If you have an external IT audit, however, these notes may not be readily available to you.

Step 4: Communicate deficiencies and implement a resolution plan.

When the IT audit is complete and the relevant deficiencies have been identified, the results and recommendations should be detailed in a clear, concise report that the IT department and management can easily understand. The appropriate supporting details and recommendations for remediation should be included. Also, risk-rating the issues can help ensure that resources are streamlined and the riskiest items are prioritized.

Next, take these steps to ensure each deficiency and recommendation is addressed:

- Have management define the anticipated resolution date for each deficiency and who will be responsible for it. Without clear ownership, issues are likely to be left unresolved or not resolved in a timely manner.
- Establish procedures for following up to ensure each deficiency is addressed and escalating unresolved issues to the appropriate management level.
- If you were an internal auditor, advocate for devoting additional resources needed to achieve resolution. By doing so, you can become the partner that your IT department needs to resolve deficiencies.

When designed and conducted appropriately, an IT audit can help strengthen your organization's cybersecurity defenses and reduce your risk.

If you have any questions about IT audits or would like to learn how we can help you with IT audits, please contact us at cybersecurity@capincrouse.com.

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 assessment, 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.