CAPINTECH

Do You Have the Right IT Controls in Place for Your Audit?

By Allison Davis Ward, Partner

Many organizations often view IT controls and processes as independent from other departments or functions. But while the IT function is a separate department with its own responsibilities and processes, **it's important to recognize that IT now touches every aspect of your environment, including financial operations.**

Today's financial teams rely on dedicated accounting servers, staff workstations, online systems, and payment processors — all of which have cybersecurity risks and considerations. With IT affecting financial operations so heavily, organizations need to view IT and cybersecurity as organization-wide concerns influencing every employee, department, and process — including financial statement audits.

The Potential Impact of IT Controls On Your External Audit

External auditors consider IT controls and processes and how they could affect the completeness and accuracy of an organization's financial statements. This includes firewalls, intrusion detection and prevention systems, internal and external vulnerability scans, patching, anti-malware protection, backup procedures, and more. And the questions external auditors ask about these controls and processes will continue to evolve as the technology supporting organizations' financial operations becomes more complex.

It's imperative for your organization to understand the implications your IT environment can have on your external audit and how deficiencies could affect your financial statements. Here are a few ways weak IT controls could, depending on severity, allow for exploitation and ultimately increase the risk of misstatement:

- Some cyber attacks are purely to **wreak havoc**. For example, an attacker who gains access to a network may simply delete data. If this happens and your organization has inadequate backup controls, you may be unable to present complete and accurate financial data.
- Some attacks aim to **disrupt operations**. If the disruption hinders your accounting team's ability to record complete and accurate financial data, there may be an impact on your financial statements.
- Many attackers aim to **steal sensitive information** they can sell on the dark web or other malicious websites. Depending on where your organization, employees, and constituents are located, you may need to comply with laws and regulations such as the Gramm-Leach-Bliley Act (GLBA), California Consumer Privacy Act (CCPA), and the European Union's General Data Protection Regulation (GDPR). If there's the potential that data was compromised, there may be financial consequences related to breach notification, legal fees, and penalties. Depending on the size of the breach, this financial impact could be material and would need to be disclosed appropriately.

While a lack of controls in a specific area could affect your organization, it does not necessarily mean that there is a material misstatement or a control deficiency. There may be other controls that mitigate the risks or assist you in recreating or recapturing data.

That's why it is important for IT controls to be designed in layers so that if one fails, additional controls are available to mitigate the impact. The more controls in your layered framework, the more likely you are to mitigate the risks successfully.

Key IT Controls to Assess at Your Organization

Important controls to evaluate within your organization include:

- **Perimeter security** – Perimeter security controls are often the first line of defense against threats from the outside world. Just like securing your home, you

External auditors consider IT controls and processes and how they could affect the completeness and accuracy of an organization's financial statements.

should secure your network entrance to prevent attacks and detect them quickly if they do occur. Organizations that maintain a physical office need two baseline perimeter security controls: firewalls and intrusion detection and prevention capabilities.

- **Vulnerability management** – Managing network vulnerabilities involves identifying the risks and then mitigating them to prevent exploitation. Vulnerability scanning, penetration testing, and patch and anti-malware management are all critical vulnerability management processes.
- **Backup management and disaster recovery planning** – Many organizations don't realize that facets of these controls can affect the availability of the data needed for your external audit. It's crucial to maintain successful backups to ensure that your data can be recovered after file corruption, system failure, ransomware, or another disaster situation. And establishing a comprehensive business continuity and disaster recovery plan is critical to ensuring continued operations and the ability to recover financial data during a disaster.
- **Application controls** – While password controls are still vital, additional layers of security such as complex and layered account lockout and multi-factor authentication (MFA) controls are becoming increasingly important and should be implemented on all financial applications, with similar configurations enabled for remote access systems.

Practical Insight and Steps

Our free CapinTech e-book, How Weak IT Controls Can Affect Your Financial Statement Audit, provides real-world examples, best practices, and practical steps to help your organization develop a greater understanding of how IT controls should be implemented and the steps you can take to build and enhance your control framework.

You'll learn how a lack of control in various areas could affect your organization, your financial data and systems, and your external audit. We also discuss the challenges many organizations face when trying to implement the critical controls listed above and provide steps and considerations your organization can take to achieve full compliance with them.

Download your free e-book today at capincrouse.com/it-controls.

If you have any questions about IT controls at your organization and how they may affect your financial statement audit, please contact us at cybersecurity@capincrouse.com. We are here to help.

About the Author

Allison Davis Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services for nonprofit organizations, financial institutions, health facilities, educational institutions, and a variety of other organizations. She stays current on changing threats to design review procedures to aid clients in implementing appropriate controls to protect against evolving cybersecurity threats. Allison speaks on information security topics for various banking, state CPA, and non-profit societies.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, 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.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA