Strengthening IT Security: One Nonprofit's Journey to Meet SAS 145 Requirements

In response to growing IT and cybersecurity risks, auditors are placing greater scrutiny on IT risk and risk controls in their audit process. The Auditing Standards Board issued a new Statement on Auditing Standards (SAS 145) that provides a more detailed risk evaluation framework and takes effect for all audits ending on or after December 15, 2023 (read more information here). The auditing standard places an emphasis on the organization's ability to identify, evaluate, and mitigate risks, specifically risks relating to the use of information technology, and many nonprofit organizations are discovering that they are not adequately prepared to meet the new standard.

Challenge

A $20 million nonprofit organization with global operations received a recommendation from their auditors in the 2023 financial statement audit, identifying deficiencies in IT risk controls. Specifically, the organization lacked a formalized IT risk assessment framework.

Like many nonprofits, they use software-as-a-service applications to support critical organizational functions such as program management, donor management, accounting, email, and file sharing. Cloud-based third-party vendors adhere to security standards; however, leadership realized they needed to improve their protocols and adopt more stringent IT security practices to meet the new SAS 145 standard.

To ensure an unbiased review of their current processes and to avoid undue burden on their IT staff, the organization sought an outside risk assessment consultant. After a review of several capable vendors, they chose GRF's Risk & Advisory team, primarily because of GRF's risk assessment expertise working with nonprofit organizations.

During the planning process, GRF identified several challenges that the organization faced:

1. Informal and inadequate IT risk assessment process.
2. Insufficient policies and procedures relating to IT security.
3. Inadequate processes for continuous improvement and assessments.

Solution

To address these IT challenges, the GRF team conducted a risk assessment that covered the following areas:

1 Asset Identification & Open-Source Threat Intelligence Scan

Conducting an OSINT scan identified publicly identifiable assets, potential risks, and mitigations.

2 Baseline Risk Assessment & IT Framework Benchmarking

This step assessed current assets, documentation, and processes against the ISO 27001 (Annex A controls) IT framework to identify gaps and risks. GRF chose this framework due to its holistic approach to information security.

3 Current State Analysis

GRF identified key risk areas and gaps, including:

1. Lack of end-user awareness and formal training programs.
2. Absence of cyber risk management policies.
3. Inconsistent security controls, such as lack of MFA, access rights to applications and data security.

At the conclusion of the assessment, GRF provided the organization with tools for implementing recommended IT security policies, baseline controls from the ISO 27001 security framework, and a cybersecurity awareness training program for its employees.

They also prepared a roadmap for implementing the recommendations to meet SAS 145 requirements and evaluate IT risks. The roadmap outlined short, medium, and long-term cybersecurity goals. Immediate goals include implementing multi-factor authentication (MFA) and security training, while longer-term goals focus on policy and procedural development.

Results

After the comprehensive IT assessment, the organization now has the tools and plans in place to better mitigate risks to their IT infrastructure. Moving forward, they have enhanced their risk management and cybersecurity posture while conforming to the requirements of the new accounting standard.

GRF Can Help

At GRF, our Risk & Advisory Services team assists clients in understanding their mission-critical risks and developing practical solutions for managing them. The team consists of subject matter experts across a range of fields including, finance, accounting, fraud and forensic auditing, information technology and cybersecurity, and U.S. government funding compliance – enabling us to provide a holistic approach to your systems assessment projects. We keep abreast of state-of-the-art industry trends and best practices, maintaining industry certifications in a broad range of risk fields, including internal audit, enterprise risk management, cybersecurity, information systems, and fraud investigations.

CPAs & ADVISORS

Risk & Advisory Services

301-951-9090

www.grfcpa.com/accounting-services/advisory-services/

For more information, contact us online, or reach out to our experts.

Mac Lillard, CPA, CIA, CFE, CISA, CRISC, CITP
Senior Manager,
Risk & Advisory Services
mlillard@grfcpa.com

Darren Hulem, CISA, CEH, Security +
Manager,
Risk & Advisory Services
dhulem@grfcpa.com

Thomas Brown, CISA, CIA, Security+, CAPM
Senior Analyst,
Risk & Advisory Services
tbrown@grfcpa.com