Texas Council Risk Management Fund

MAINTAINING INTERNAL CONTROLS AND POLICIES

In today's digital environment, maintaining strong internal controls and well-defined policies is more critical than ever. As organizations embrace cloud computing, remote work, and automation, the risk landscape has expanded, introducing new cybersecurity threats alongside traditional operational and financial risks.

Internal controls are no longer limited to finance and compliance—they now play a central role in protecting data, systems, and organizational reputation.

Why Maintenance Matters

Internal controls must evolve to keep pace with rapidly changing cyber risks. Controls that were effective a year ago may no longer protect against modern threats like ransomware, phishing, or insider attacks. Risk mitigation remains the fundamental purpose of internal controls, but the scope has expanded beyond traditional financial oversight. Controls now address operational risks, technology vulnerabilities, supply chain disruptions, and regulatory changes that can impact business continuity and growth trajectories.

Maintaining controls ensures they remain:

- Aligned with evolving cyber threats
- Effective across digital environments
- Resilient against both internal and external risks

Building a Strong Control Environment

Leadership sets the tone for both compliance and cybersecurity awareness. A culture of accountability and security-minded behavior is essential. Internal controls provide the foundation for implementing complex business processes across growing organizations. When controls are embedded into workflows, employees understand expectations and can engage with systems and data securely while supporting strategic initiatives.

Continuous Risk Assessment

Cyber risks are dynamic and must be reassessed frequently. The risk assessment process is conducted to identify and analyze risks to achieving objectives and helps form a basis for managing risks. Objectives must be clearly defined for a risk assessment to be most effective. When assessing risks, management should consider changes in the external business environment, internal business model, and the potential for fraudulent activities.

- Regularly assess risks related to patient data breaches and ransomware targeting hospitals.
- Evaluate processes related to employee, client, or vendor account changes.
- Evaluate risks of payment card fraud and data breaches affecting customer information.
- Conduct vulnerability scans and penetration testing
- Assess third-party/vendor cybersecurity risks

- Monitor emerging threats (e.g., zero-day vulnerabilities)

Regular Monitoring and Testing

Continuous monitoring is critical for both operational and cybersecurity controls. Management should establish appropriate control activities, as well as employee expectations in performing these activities, in all policies and relevant procedures to help ensure management's directives to mitigate risks are carried out. Control activities are performed at all levels, at various stages of business processes, and over technology. These activities include, but are not limited to, segregation of duties, timely reconciliations, and supervisory review. Monitoring internal controls should be ongoing, with identified weaknesses or deficiencies communicated in a timely manner. Deficiencies that are more serious in nature must be reported to senior management and the board. Corrective actions must also be regularly monitored to ensure they are implemented timely and effectively.

- Security Operations Centers (SOCs) monitor logs and alerts 24/7
- Monitor point-of-sale systems for unauthorized access or malware

Updating Policies and Procedures

Cybersecurity policies must evolve alongside threats and regulations. Internal controls are dynamic, not static. Continuously monitor their effectiveness, identify areas for improvement, and implement necessary changes. This ensures your controls stay relevant and adapt to your evolving business needs.

- Acceptable Use Policies (AUP): Define how employees access systems and data
- Incident Response Plans: Regularly updated to address emerging attack methods
- Data Protection Policies: Revised to align with regulations like HIPAA
- Review audit findings and cyber incidents
- Update controls based on threat intelligence

Benchmark against frameworks like:

- COSO (Internal Controls)
- NIST Cybersecurity Framework
- ISO 27001

Training and Awareness

Human error remains one of the leading causes of control failure, especially in cybersecurity. Empower your employees to be active participants in upholding internal controls. Provide ongoing training on your control procedures, their importance, and how to identify and report potential breaches.

- Employees trained in protecting organizational property from cyber espionage
- Conduct phishing simulation exercises to improve awareness
- Make cybersecurity training ongoing—not just annual
- Use real-world attack simulations
- Tailor training to employee roles

Common Pitfalls to Avoid

Internal controls are highly effective, but they're not infallible. Inherent limitations of internal controls exist, but by identifying them, organizations can work through them and find mitigation strategies. Here are some common areas that can cause failure in controls.

- Treating cybersecurity as separate from internal controls
- Lack of segregation of duties
- Over-reliance on manual controls in high-risk digital environments
- Infrequent access reviews
- Lack of incident response readiness
- Failure to address third-party/vendor risks

Final Thoughts

Maintaining internal controls in today's environment means integrating cybersecurity into the core of governance and risk management. Organizations that take a proactive approach—combining strong policies, advanced technology, and continuous monitoring—are better equipped to protect their assets and maintain stakeholder trust. Internal controls must evolve beyond finance—cybersecurity is now a critical component.

The TCRMF Cyber Risk Services Advisor has started to schedule Incident Response Plan Tabletop Testing visits for members. To be included on the schedule, contact Lee Cain, Cyber Risk Services Advisor, at 512-619-1437 or Lee.Cain@sedgwick.com.