Recent updates from the SEC which impact Internal Audit
November 30, 2018
Recent updates from the SEC which impact Internal Audit
Recent updates from the SEC which impact Internal Audit

Cyber

a

b

SOC for Cyber

RPA

a

Auditing RPA
Recent updates from the SEC which impact Internal Audit

A. SEC Investigative Report:
   a. Internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds.
   b. Public issuers subject to the requirements of Section 13(b)(2)(B) must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly.
   c. Given the prevalence and continued expansion of these attacks, issuers should be mindful of the risks that cyber-related frauds pose and consider, as appropriate, whether their internal accounting control systems are sufficient to provide reasonable assurances in safeguarding their assets from these risks.

B. GITCs
   a. MFA
   b. VPN
   c. Encryption of email
   d. URL filtering
   e. Endpoint security

C. Business controls
   a. Authorization verification controls
   b. Review of vendor or employee master file changes
   c. Change confirmation
Cyber—SOC for Cyber

Cyber examination background
On April 24, 2017, the American Institute of Certified Public Accountants (AICPA) released its cybersecurity risk management attestation reporting framework. This framework establishes a standardized reporting mechanism to provide a broad range of users with useful information about an entity’s cybersecurity risk management program.

Key stakeholders
- Board of directors
- Regulators
- Cyber insurance carriers
- Customer

AICPA cybersecurity attestation reporting framework
1. Management’s description of the cybersecurity risk management program
2. Management’s assertion on:
   • The presentation of the description
   • The operating effectiveness of the controls to achieve the cybersecurity objectives
3. Practitioner’s opinion on:
   • The presentation of the description
   • The operating effectiveness of the controls to achieve the cybersecurity objectives

Benefits
- Greater transparency
- Independent and objective reporting
- Operational efficiencies
- Useful in making informed and strategic decisions
- Strategic competitive advantage and enhancement to brand and reputation
- A comprehensive set of criteria/control framework(s)
Auditing RPA

- Reliance on pre implementation SDLC controls
- Benchmarking RPA
- Testing RPA as automated controls
Questions