Ten Emerging Information Technology (IT) Audit Issues

October, 2015
Overview

- IT controls continue to increase in importance to organizations
- Corporate reliance on technology increases
- Compliance requirements increase
- Deficiencies in IT controls can have a significant impact on the organization
Risk landscape

Today’s risks
• Cyber security/data breaches/state-sponsored attacks
• Third-party risk management
• Data protection/data loss prevention
• Social media
• Data analytics/data mining/data visualization

Tomorrow’s risks
• Wearable technologies
• Drone technologies
• Cognitive computing
• Open source solutions (Hadoop, Mahout, Spark)
• Sensor proliferation
Today’s risks: Cyber security

Issue
Cyber continues to increase in importance, and new cyber standards have emerged. Significant increase in cyber activities and breaches; heightened attention from boards, audit committees, customers, partners, employees, auditors and regulators. Historic internal audit cyber reviews may provide insufficient coverage.

Risk
Direct loss of money.
Impact to organizational brand.
Loss of critical or confidential data.
Fines, sanctions.

Recommendation
Move from thinking about project audits to program audits. Perform a thorough cyber risk assessment, covering all aspects of cyber (secure, vigilant, resilient). Components of an effective cyber program should be highly integrated, programmatic, and extend beyond the walls. Define multi-year audit plan covering all cyber domains. Execute audits along defined schedule.
Today’s risk: Third-party risk management

Issue
Increased focus on use of third parties or Outsourced Service Providers (OSP) for technology and/or support solutions. Ease of procurement for third-party solutions, particularly point specific cloud solutions. COSO 2013 requirement for management of OSPs.

Risk
Lack of understanding of what data and solutions are currently provided by OSPs
SOC 1 reports do not provide enough coverage
Loss of critical business data
Lack of effective controls

Recommendation
Understand organization’s current population of OSPs where key internal controls have been outsources. Obtain SOC 1 reports if possible. Evaluate the user controls considerations and perform tests of controls. Evaluate the effectiveness of organization’s monitoring procedures over control activities performed by OSPs. Evaluate how expectations for integrity and ethical values have been communicated to OSPs.
Today’s risk: Data protection / data loss prevention

**Issue**
Increased scrutiny of data lifecycle management by regulators, auditors, customers, employees and business partners. Issue is exacerbated due to device proliferation, cloud support, emerging malware technologies, evolving regulatory requirements, and file sharing solutions.

**Risk**
- Fines, financial impacts
- Loss of brand
- Loss of critical data

**Recommendation**
Move to a programmatic approach to auditing, similar to cyber risk. Point specific issues are no longer helpful. Begin with organization policies and taxonomies. Review linkages to relevant laws and regulations. Evaluate storage and defensible destruction requirements. Evaluate linkage to bring-your-own-device management policies and procedures.
Today’s risk: Social media

Issue
Significant deployment of social media solutions and technologies as critical business drivers, i.e., social business. Rapidly evolving technologies with commensurate rapidly evolving regulatory requirements and risk. Ease of deployment may hamper visibility of solutions in place to management. Businesses need to consider personal use as well.

Risk
Loss of brand reputation
Exposure to regulatory sanctions and/or fines
Legal liabilities such as copyright or trademark infringement
Financial disclosures risk

Recommendation
Move from thinking about project audits to program audits. Program audits should encompass all aspects of social media within the organization, including integration points, crisis management plans, and relevant regulatory requirements. Consider legal aspects, including development of policies and procedures and human resource activities.
Today’s risk: Data analytics

**Issue**
Increased utilization of data analytic technologies to provide governance, risk and control activities across all three lines of defense. Shifts business decision making from retroactive reviews to predictive modeling and real time alerts.

**Risk**
Data inaccuracies may have larger impacts
Analytic failures may have larger impacts
May impact overall control environment
Increased data lifecycle risk (e.g., personally identifiable information)

**Recommendation**
Define analytics strategy for supporting internal audit activities (beyond structured queries). In addition, determine the extent of analytic technologies (either deployed or in-process) throughout the organization. Risk assess the data, processes and decision making driven off of these. Plan audit procedures accordingly. Consider completeness and accuracy of data stores.
Tomorrow’s risks: Wearable technologies

**Issue**
Wearable technologies (glasses, watches, bracelets, smart badges) is migrating from consumer space to business, impacting how employees, customers and partners interact.

**Risk**
Three functions (sensing, display, computing) may be distributed.
Data transmission may contain sensitive information.
May represent the initial event for event driven processing.
Lack of industry standards.

**Recommendation**
Inventory and assess current wearable initiatives. Determine types of data processed and events initiated. Risk rank appropriately and then define audit procedures accordingly.
Tomorrow’s risks: Drone technologies

**Issue**
Rapid evolution of guided and non-guided vehicles for business application. Can serve a variety of purposes, more than just supply chain applications. Potential for significant disruption. Lack of standards or regulatory oversight.

**Risk**
Regulatory violations
Potential for physical events (crashes, loss of life)
Potential cyber exposure
Potential need for guidance (radio waves, perimeter devices)
Lack of qualified support resources

**Recommendation**
Tomorrow’s risks: Open source technologies

Issue
Open source technologies are now finding large scale use in organizations, particularly for infrastructure elements. Often use of open source solutions may be unknown to executive management.

Risk
Security risks
Ease of modification
Support
Reliance on personnel, internal and external
Vulnerability to intellectual property claims and other legal issues

Recommendation
Determine extent of current open source use throughout the organization. Assess level of customization and security. Assess patching and security processes. Assess usage alignment with relevant licensing terms.
Tomorrow’s risks: Cognitive computing

Issue
Cognitive computing platforms and technology is becoming more prevalent, and will be the driving factor behind real time critical decision making for a variety of business purposes, including risk management, buy/sell decisions, retail and health care. Solution providers are making large investments in exploring business applicability, and we should expect an evolving array of offerings, including self driven apps. May also be the governance, risk and control model of the future third line of defense.

Risk
Requires good data management and real-time data feeds
Poor management of solutions could drive poor decision making, which may be automated
Loss of brand reputation

Recommendation
Understand current and planned use of cognitive technologies within the organization.
Determine what decisions will be driven off of cognitive platforms. Assess risk commensurate with planned usage, including data management. Consider applications within third line of defense as well.
Tomorrow’s risks: Sensor proliferation

**Issue**
Rapid expansion of distributed sensor nodes, which in turn help drive and/or control business events. May or may not be connected to the Internet of Things (IoT).

**Risk**
Effective management of very large numbers of sensors
Effective data usage processes and policies
Variety of risks related to inoperable sensors
Potential increased cyber exposure

**Recommendation**
Develop understanding of current and planned deployment of sensor technologies with your environment. Evaluate risks based on type of sensor and planned usage and design corresponding consultative and assurance procedures.
Summary

Determine which items may be relevant in your business and technical environment

Ensure that risk assessment and audit universe address relevant items

Collaboration and communication with IT, audit committee and other stakeholders is key

Plan resource requirements:
• Be careful not to underestimate
Contact information

Stuart Rubin
Director, Deloitte & Touche LLP
954-899-4407

stuartrubin@deloitte.com

www.linkedin.com/pub/stuart-rubin/1/62b/374