Top Ten Information Technology (IT) Internal Audit Issues - 2016

Michael Juergens
CISA, CRISC, CGEIT, CSXF, CIA, CGAP, CRMA
Principal
Deloitte & Touche LLP
Contents

IT Internal Audit Universe 4
Cyber Assurance 5
Drone Technologies 6
Third-party Management 7
Alternative Workforce 8
Virtual Reality 9
Sensor Proliferation 11
Payment Systems 12
Data Management/Data Governance 13
Artificial Intelligence 14
Disaster Recovery and Resilience 15
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
IT Internal Audit Universe
Cyber Assurance

Issues
• Cybersecurity risks are being managed by enterprise programs.
• They require an assurance component currently lacking in many organizations.
• Evolving standards and regulations (e.g., Federal Financial Institutions Examination Council (FFIEC), Securities & Exchange Commission (SEC)) will make this a critical component of internal audits going forward.

Risks
• Direct loss of money
• Impact to organizational brand
• Loss of critical or confidential data
• Fines and/or sanctions

Recommendations
• Internal Audit needs a cyber assurance strategy.
• Must be programmatic and comprehensive.
• Must be ongoing and planned over a multi-year assurance cycle.
• Staffing considerations are critical.
Drone Technologies

Issues
- 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

Risks
- 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

Recommendations
- Monitor evolution of solutions.
- Discuss with management planned explorations of solutions.
- Perform detailed risk analysis of planned explorations.
- Work with management to develop control solutions.
Third-Party Management

Issues
• Increased reliance on 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

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

Recommendations
• Understand organization’s current population of third-party providers.
• Move from microfocus on risk areas to evaluate third-party management governance.
• Consider operational and reputational risk factors (quality, performance), charging, and legal/regulatory risk.
• For specific risk areas, obtain SOC 1 reports if possible and understand gaps.
Alternative Work Force

Issues
• Employee-based workforce model is rapidly becoming obsolete.
• Replaced by contractors and challenge-based workforce solutions.
• Creates security, intellectual property (IP), platform consistency, and other issues.

Risks
• Loss of critical business data
• Component integration challenges
• Nonadherence to corporate standards
• Security vulnerabilities

Recommendations
• Understand current workforce models.
• These will not all go through human resources.
• Develop and execute comprehensive work plan, including policies and procedures, provisioning/deprovisioning, onboarding, IP requirements, platform management, and topical issues.
Virtual Reality

Issues
• Virtual reality technologies have arrived.
• Primarily consumer-based (e.g., smart glasses, smart phones).
• Moving into business-oriented applications.
• Potentially transformational.

Risks
• Full scope unknown
• Potential loss of data
• Failure to adapt
• Evolving control structure

Recommendations
• Discuss with application development team any potential movement toward virtual reality applications.
• Understand scope and functionality presented to determine risk profile and impact on controls.
• Define audit procedures.
• Consider impact on system development life cycle.
Sensor Proliferation

Issues
• 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).

Risks
• 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

Recommendations
• Develop an understanding of current and planned deployment of sensor technologies within your environment.
• Evaluate risks based on type of sensor and planned usage and design corresponding consultative and assurance procedures.
Payment Systems

Issues
• Rapid technology shifts in non-cash alternative payment solutions, from contactless and mobile transactions to alternative currency options
• Forces regulatory and process changes, as well as customer-facing issues

Risks
• Exposure to cyber attack
• Regulatory requirements
• Inability to manage cash effectively
• Privacy laws

Recommendations
• Need to evolve internal audit procedures to address emerging risks.
• This could include regulatory risk assessment, security assessments, review of payment projects, assessment of current solutions, and impacts on Sarbanes-Oxley compliance.
Data Management/Data Governance

Issues
• Increased scrutiny of data life cycle 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

Risks
• Fines, financial impacts
• Loss of brand
• Loss of critical data

Recommendations
• 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.
Artificial Intelligence

Issues
• Cognitive computing technology is becoming more prevalent, and will likely 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.
• Many solution providers are making large investments in exploring business applicability.
• Evolving array of offerings, including self-driven apps.
• May become the future third line of defense.

Risks
• Requires good data management and real-time data feeds
• Poor decision making, which may be automated
• Loss of brand reputation

Recommendations
• 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.
Disaster Recovery

Issues
• As automation increases, and the extended enterprise becomes more complex, resilience becomes increasingly difficult to manage effectively.
• Many instances of failures emerged in 2015 despite increased focus in this area.

Risks
• Loss or corruption of data
• Brand and customer impacts
• Regulatory impacts

Recommendations
• Evolve the internal audit approach to auditing resiliency and disaster recovery.
• Broaden the focus of internal audit procedures to determine the adequacy of processes in place to avoid, respond, and recover from outages.
• Consider nontechnical components such as communication and public relations.
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 are key.
- Plan resource requirements.
- Be careful not to underestimate.
Contact Information

Michael Juergens
Principal, Deloitte & Touche LLP
213-688-5338

michaelj@deloitte.com
www.linkedin.com/pub/michael-juergens/2/221/988
@michaeljuergens
This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2016 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited