The Changing IT Risk Landscape
Understanding and managing existing and emerging risks

IIA @ Noon

Kareem Sadek
Senior Manager, Deloitte Canada

Chris Close
Senior Manager, Deloitte Canada

December 2, 2015
Agenda

- Current IT risk landscape
- Evolving IT internal audit universe
- Today’s IT risks
- Tomorrow’s IT risks
- Tools for today’s internal auditor
- Discussion and closing thoughts
Current IT Risk Landscape
Current IT Risk Landscape

Deficiencies in IT controls can have a significant impact on the organization.
Evolving IT Internal Audit Universe
Evolving IT Internal Audit Universe

The IT internal audit areas listed below help you adapt your IT audit plan to be more relevant, forward thinking, and emerging risk focused.

Characteristics of services

<table>
<thead>
<tr>
<th></th>
<th>Core</th>
<th>Advanced</th>
<th>Emerging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Derived client value</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Complexity of technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject matter expert requirement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource cost</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>India offshore staffing opportunity</td>
<td></td>
<td>〇 〇 〇</td>
<td></td>
</tr>
<tr>
<td>Compliance risk oriented</td>
<td>〇 〇 〇</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategic risk oriented</td>
<td></td>
<td>〇 〇 〇</td>
<td></td>
</tr>
<tr>
<td>Current portion of IT IIA plan</td>
<td>〇 〇 〇</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 〇 = High
- 〇 = Medium
- 〇 = Low
Evolving IT Internal Audit Universe
Risk landscape

Today’s IT risks
• Cybersecurity
• Third-party risk management
• Cloud computing
• Mobile device governance
• Social media

Tomorrow’s IT risks
• Drone technologies
• Open source solutions
• Cognitive computing
• Sensor proliferation
Today’s IT risks
Today’s IT risks
Cybersecurity

Issue
• Cyber continues to increase in importance, and new cyber standards have emerged. There has been a 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 IT risks
Cybersecurity Framework

<table>
<thead>
<tr>
<th>Secure</th>
<th>Cybersecurity risk and compliance management</th>
<th>Secure development life cycle</th>
<th>Security program and talent management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Compliance monitoring</td>
<td>Secure build and testing</td>
<td>Security direction and strategy</td>
</tr>
<tr>
<td></td>
<td>• Issue and corrective action planning</td>
<td>• Secure coding guidelines</td>
<td>• Security budget and finance</td>
</tr>
<tr>
<td></td>
<td>• Regulatory and exam management</td>
<td>• Application role design/access</td>
<td>management</td>
</tr>
<tr>
<td></td>
<td>• Risk and compliance assessment and migrat.</td>
<td>• Security design/architecture</td>
<td>• Policy and standards management</td>
</tr>
<tr>
<td></td>
<td>• Integrated requirements and control</td>
<td>• Security/risk requirements</td>
<td>• Exception management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Talent strategy</td>
</tr>
<tr>
<td></td>
<td>Third-party management</td>
<td>Information and asset</td>
<td>Identity and access management</td>
</tr>
<tr>
<td></td>
<td>• Evaluation and selection</td>
<td>management</td>
<td>• Account provisioning</td>
</tr>
<tr>
<td></td>
<td>• Contract and service initiation</td>
<td>• Information and asset</td>
<td>• Privileged user management</td>
</tr>
<tr>
<td></td>
<td>• Ongoing monitoring</td>
<td>classification and inventory</td>
<td>• Access certification</td>
</tr>
<tr>
<td></td>
<td>• Service termination</td>
<td>• Information records</td>
<td>• Access management and governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Physical and environment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>security controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Physical media handling</td>
<td></td>
</tr>
<tr>
<td>Vigilant</td>
<td>Threat and vulnerability management</td>
<td>Data management and protection</td>
<td>Risk analytics</td>
</tr>
<tr>
<td></td>
<td>• Incident response and forensics</td>
<td>• Data classification and</td>
<td>• Information gathering and analysis</td>
</tr>
<tr>
<td></td>
<td>• Application security testing</td>
<td>inventory</td>
<td>around:</td>
</tr>
<tr>
<td></td>
<td>• Threat modeling and intelligence</td>
<td>• Breach notification and</td>
<td>• User, account, entity</td>
</tr>
<tr>
<td></td>
<td>• Security event monitoring and logging</td>
<td>management</td>
<td>• Events/Incidents</td>
</tr>
<tr>
<td></td>
<td>• Penetration testing</td>
<td>• Data loss prevention</td>
<td>• Fraud and anti-money laundering</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability management</td>
<td>• Data security strategy</td>
<td>• Operational loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data encryption and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>obfuscation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Records and mobile device</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>management</td>
<td></td>
</tr>
<tr>
<td>Resilient</td>
<td>Crisis management and resiliency</td>
<td>Security operations</td>
<td>Security awareness and training</td>
</tr>
<tr>
<td></td>
<td>• Recover strategy, plans, and procedures</td>
<td>• Change management</td>
<td>• Security training</td>
</tr>
<tr>
<td></td>
<td>• Testing and exercising</td>
<td>• Configuration management</td>
<td>• Security awareness</td>
</tr>
<tr>
<td></td>
<td>• Business Impact analysis</td>
<td>• Network defense</td>
<td>• Third-party responsibilities</td>
</tr>
<tr>
<td></td>
<td>• Business continuity planning (BCP)</td>
<td>• Security operations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Disaster recovery planning (DRP)</td>
<td>• Management</td>
<td></td>
</tr>
</tbody>
</table>

* The Deloitte cybersecurity framework is aligned with industry standards and maps to NIST, ISO, COBIT, and ITIL.

SOX (financially relevant systems only)

Penetration and vulnerability testing

BCP/DRP testing
Today’s IT risks

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 outsourced. 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 IT risks
Cloud computing

Issue
• The use of cloud services may impact and change IT and Business risks. Organizations benefit from a risk-based, governance program to manage the range of areas impacted by the cloud, including on-premise activities to hybrid and multi-cloud scenarios that aligns with the business strategy.

Risk
• Lack of a specific cloud computing strategy and standard
• Changes required for roles, responsibilities, documentation, and process enhancements
• Requests for numerous audits and assessments targeting vendors and cloud providers
• Determining where control ownership truly resides “in the cloud”

Recommendation
• Develop a profile of the cloud computing environment in use by the organization. Based on the cloud use profile, evaluate through review and interviews with process owners, each of the cloud risk domains to identify specific risks the cloud environment may have to the organization. Perform a gap analysis and evaluate the maturity of each of the listed domains.
Today’s IT risks
Cloud Approach

Governance, risk management, and compliance
- Review and assessment of management’s policies and procedures in place to evaluate and monitor cloud adoption and usage
- Review and assessment of whether management has built a comprehensive risk management cloud strategy that:
  - Formulates a risk management road map for cloud
  - Probes impact of risk events
  - Prioritizes risk mitigation activities
- Review and assessment of management’s current approach to manage changes and monitor compliance with regulatory requirements

Vendor management
- Review and assessment of management’s vendor selection process and controls.
- Review and assessment of management’s vendor contracting process and controls (i.e. involvement of legal, HR and procurement where necessary).
- Review and assessment of management’s resource provisioning and monitoring of cloud vendors
- Review and assessment of management’s process and controls to avoid vendor lock-in.

Business operations
- Review and assessment of management’s process and controls to ensure that the right resources and departments are involved in the cloud process when and if needed
- Review and assessment of management’s process and controls in place to ensure that the right resources are trained and available to manage the cloud based technologies. Only appropriate users having access to administrative cloud access.
- Review and assessment of management’s process and controls in place to ensure that proper legal (e.g. retention of documents) and financial (e.g. documentation of financial controls) cloud considerations are in place.
Today’s IT risks
Mobile device governance

Issue
• Organizations must consider the security of mobile devices, applications, and related infrastructure systems, such as mobile data management (MDM). Integration of mobile systems with existing enterprise solutions, such as Active Directory, Security Incident, and Event Management, and Data Loss Protection, is a challenge in today’s IT environment.

Risk
• No concrete regulatory requirements developed for mobile applications
• Sustaining security management in the face of evolving technology and threats
• Increasing risk and liability associated with breaches
• No control on the mobile device in the case of bring your own device (BYOD) scenario
• Heightened awareness and concerns about privacy

Recommendation
• Review and assess mobile security strategy; that address multiple regulatory/legal requirements. Review and assess mobile security policies, procedures, and guidelines, and review and assess training/awareness to users; and periodic monitoring and reporting.
Mobile device governance - Approach

<table>
<thead>
<tr>
<th>Element</th>
<th>Key considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activation</td>
<td>What is the process for enabling a new employee with a device?</td>
</tr>
<tr>
<td>Device management</td>
<td>How will devices be remotely managed? What level of centralized control will exist?</td>
</tr>
<tr>
<td></td>
<td>What level of management will be done at the end-point (e.g., containerization)?</td>
</tr>
<tr>
<td></td>
<td>How will devices be locked, wiped and restored?</td>
</tr>
<tr>
<td>Lost/stolen device</td>
<td>What happens when a device is lost, stolen or damaged?</td>
</tr>
<tr>
<td>Support</td>
<td>What kind of support, and how much support, can a user expect from your organization?</td>
</tr>
<tr>
<td>Acceptable use</td>
<td>What kinds of devices, platforms, applications, services and accessories are allowed under the BYOD program?</td>
</tr>
<tr>
<td>Reimbursement</td>
<td>Who pays for the initial device? What level of stipend is available? Is it consistent across all eligible users? Is it available recurrently?</td>
</tr>
<tr>
<td>Privacy</td>
<td>How will employee privacy be protected? Will your support group have access to personal information?</td>
</tr>
<tr>
<td>Policy violations</td>
<td>How will policy violators be dealt with? Will BYOD policies contradict or conflict with other policies (e.g., HR policies for employee responsibilities, overtime, etc.)</td>
</tr>
<tr>
<td>Eligibility</td>
<td>Who is eligible for the BYOD program? What roles, levels, etc. are eligible and in what way (e.g., tiered eligibility)?</td>
</tr>
</tbody>
</table>

Use understanding to define areas in scope

Mobile program governance
- Review and assessment of current Mobile strategy: Determine whether a strategy document exists to outline the company’s roadmap for using mobile devices.
- Review and assessment of defined roles and responsibilities for mobile operations and security. Review and assessment of Mobile use/acceptable use policy: Determine whether an acceptable use policy exists to define the permitted and prohibited usage of devices.
- Review and assessment of training and awareness programs: Determine whether training modules and documentation are defined in order to train end users on mobile device/application acceptable usage and security in accordance with Enterprise security policies and standards. Determine whether training is updated and conducted on a regular basis to keep users aware of any changes to the defined policies around mobile devices to ensure compliance.

Mobile device security & configuration
- Review and assessment of device provisioning, tracking/inventory and decommissioning controls: Assess whether a process for device commissioning and decommissioning is defined and documented.
- Review and assessment of secure configuration requirements and standards.
- Review and assessment of controls in place to manage software/firmware updates that affect security i.e. a patch management process exists for devices to patch or upgrade the device OS and applications.

Data protection and incident response
- Review and assessment of permissible data storage policies as defined by acceptable use policy.
- Review and assessment of encryption policies and controls.
- Review and assessment of secure data transmission policies and controls.
- Review and assessment of the incident response strategy in place.

Deloitte – Transforming IT Internal Audit | © Deloitte LLP and affiliated entities.
Today’s IT risks

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.
Tomorrow’s IT risks
THIS IS 1999
Tomorrow’s IT 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

Open Source Technologies

**Issue**
- Open source technologies are now finding large scale use in organizations, particularly for infrastructure elements. Use of open source solutions may often 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
Tomorrow’s IT risks

Cognitive Computing

Issue
- Cognitive computing platforms and technology are 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. 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

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
Tools for today’s internal auditor
Tools for Today’s Internal Auditor

Data analytics

- Define analytics strategy for supporting internal audit activities (beyond structured queries).
- 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.
Discussion and closing thoughts
Discussion and closing thoughts

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

2. Ensure that risk assessment and audit universe address relevant items

3. Collaboration and communication with IT, audit committee and business and corporate areas are key

4. Plan resource requirements:
   - Be careful not to underestimate
For more information
Your presenters

Kareem Sadek
Sr. Manager, Enterprise Risk Services
416-775-7268
ksadek@deloitte.ca

Chris Close
Sr. Manager, Enterprise Risk Services
613-751-5276
cclose@deloitte.ca
Deloitte, one of Canada’s leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

The information contained herein is not intended to substitute for competent professional advice.