Auditing Risk of Disruptive Technologies
The IIA Edmonton Chapter
JANUARY 21, 2021
Contents

01 Introduction

02 Understanding Digital Transformation

03 Key Risks

04 Approaches to Auditing Disruptive Technologies

05 Q&A
About Us

Baskaran Rajamani

Baskaran leads Technology and Digital Risk services for Deloitte in Canada. In this role he helps clients transform how they manage and govern risks related to conventional IT as well as a whole range of disruptive Technologies like Automation, Agile, AI, Blockchain, Cloud, Cognitive, Digital etc. to enhance the efficiency, effectiveness and agility/adaptability of their Risk Management framework and operating model across three lines of defense.

Baskaran is part of Deloitte’s global team to develop methodology and thought leadership materials on disruptive technology risks and governance.

Mark Varma

Mark is a Senior Manager in Deloitte’s Risk Advisory practice. He has significant experience managing IT risk and control, IT audit and advisory engagements for Deloitte priority accounts. Mark leads Deloitte and client training on IT audit, IT controls and third-party risk.

In addition to delivering key client engagements, Mark also plays a quality assurance role on some of Deloitte’s large IT audit projects and has led development of Deloitte’s submissions on emerging IT audit topics to CPA Canada, ISACA and other organizations – including most recently on blockchain and crypto-asset assurance.
Introduction
“Going digital” is no longer an option!

Over the last three years organizations have invested in their Digital Transformation journey, in many instances, leveraging several Disruptive Technologies. The COVID-19 pandemic has further accelerated this trend.

Internal Audit should quickly understand the implications, anticipate assurance needs, and prepare to deliver while also considering its own digital transformation.
Business Examples of Digital Transformation

Loblaws rolled out the **PC Health App**, a new personalized digital health app designed to improve how Canadians access and navigate healthcare with **enhanced analytics capabilities, virtual care offerings and built-in e-commerce.**

[https://www.pchealth.ca/](https://www.pchealth.ca/)

Hospital uses **an app to screen patients’ vital signs** and monitor symptoms without touching them: heart rate, respiratory rate and oxygen saturation in the blood.

[https://www.jgh.ca/care-services/](https://www.jgh.ca/care-services/)

As demand for personalized remote exercise has grown, Lululemon acquired the in-home fitness company, Mirror, which offers **live and on-demand digital fitness classes through a smart mirrored display.**

[https://shop.lululemon.com/story/mirror-home-gym/](https://shop.lululemon.com/story/mirror-home-gym/)

Among other Digital solutions, TD rolled out **Clari, a conversational AI chatbot** to answer several common account related customer queries to reduce call-centre load.

The COVID-19 pandemic has forced businesses and governments to take advantage of a rare opportunity to experiment rapidly and extensively with new technologies as they seek to cope with the global social and economic disruption.

Disruptive technologies, like AI, digital payments, robotics, and 3D printing, are playing a key role in supporting the covid-19 response and recovery efforts.

Successful digital transformation demands risk intelligence throughout the lifecycle.
Evolution of Advanced Analytics

Where is your organization in this continuum?

Degree of Automation

- **Foundation**
  - Data Integration
    - Integrated data to provide consistent information foundation (e.g., compliance risk and regulatory data warehouse)
  - Predictive Analytics
    - Software solutions using predictive models (e.g., compliance risk models)
  - Data Visualization
    - Software placing data in a visual context
  - Robotic Process Automation (RPA)
    - Rules-based systems that mimic human behavior to automate parts of repeatable processes offering efficiency and scalability
  - Machine Learning (ML)
  - Artificial Intelligence (AI)

- **Analytics**
  - Natural Language Generation
    - Application that accept structured data inputs to generate seemingly unstructured narratives
  - Natural Language Processing
    - Application that process unstructured data to generate structured data

- **Automation**
  - Efficient back-office operations
  - Attended automation

- **Cognitive Intelligence**
  - Product recommendation
  - Chatbots
  - Cyber attack prediction

Use Cases

- Enterprise-level reporting on risk, performance and business intelligence
- Predictive analytics
- Custom demand forecasting
- Efficient back-office operations
- Attended automation
- Product recommendation
- Chatbots
- Cyber attack prediction

Business Values

- Enterprise-level reporting on risk, performance and business intelligence
- Predictive analytics
- Custom demand forecasting
- Efficient back-office operations
- Attended automation
- Product recommendation
- Chatbots
- Cyber attack prediction

Inherent risk

© Deloitte LLP and affiliated entities.
The Digital Playing Field

Each new technology brings new risks that have specific mitigation requirements.
Poll Question #1

What digital technologies have been implemented at your organization?

1. Automation & Robotics
2. Agile Development & Implementation
3. APIs
4. Cloud
5. Machine Learning
6. Internet of Things
The Digital Technologies Canvas

Impact Across Industries
- Social Media & Digital Platforms
- Robotic Process Automation
- Mobile Endpoint Devices & Apps
- Artificial Intelligence & Cognitive Computing
- Commercial drones
- Smart Contracts

Impact Across Use Cases
- Biometrics
- Conversational Computing & Virtual Assistance
- Sensors & The Internet of Things
- Blockchain
- Social Robotics
- 3D printing
- Additive manufacturing
- Autonomous Vehicles

Niche Impact
- Virtual Reality & Augmented Reality
- Human Augmentation Brain-Computer Interfaces
- Quantum computing

Maturing 0 – 2 years
Emerging 2 – 5 years
> 5 years

Auditing disruptive technologies – IIA Edmonton Chapter
Implications for Internal Audit
Key Questions from Stakeholders

Audit Committee
• Does Digital transformation impact integrity of financial reporting? Are there any SOX compliance impacts?
• Other opportunities to leverage emerging technologies for increasing efficiency, effectiveness and agility of audit?

Shareholders
• Does the entity have an independent, ongoing assessment of its privacy and security controls?
• Does the entity have a business continuity or recovery plan in the event its IT systems are disabled?

CEO and the Board
• Which digital activities, processes and functions pose the most risk exposure to our enterprise and potentially our brand and reputation?
• Are we within the risk appetite for the enterprise? How do we know?

CFO and CXOs
• Does management know and understand the cost of digital threats to our organization? Can this amount be measured?
• What are the oversight procedures on disruptive technologies to avoid high-impact operational errors?
Three Implications of Disruptive Technologies for Internal Audit
Leading internal audit functions successfully handle all three implications

1. Disruptive Technologies introduce new risks that organizations need to manage (and hence IA needs to be aware of and anticipate assurance needs).

2. Disruptive technologies challenge the existing operating model for engagement across the three lines of defense.

   What is demanded is shared understanding, more agile engagement, gaining credibility to provide real value to the first line.

3. Disruptive technologies also offer opportunities for IA itself to leverage these emerging technologies for increasing efficiency, effectiveness and agility of audit.
Sample of Digital Transformation Risk Incidents
IA functions should consider a variety of conventional and unconventional risks while auditing disruptive technologies

**Safety and reliability**

**Safety & Security**

Series of accidents involving self-driving cars has raised questions about the safety of these futuristic new vehicles, which are being tested on public roads in several American states.

**Credibility & Reliability**

Mistakes in facial recognition have impacted genuine individuals on one hand while being a security weakness on the other hand.

**Legality and regulations**

**Legal considerations**

Hiring tool discriminated against women due to the biased dataset leading to a discriminatory algorithm.

**Data Protection & Breach**

Data proliferation and access channels associated with Digital products and services caused hacks and compromise of client data leading to privacy breaches.

**Ethics and reputation**

**Ethical concerns**

Microsoft’s Tay chatbot experiment went disastrous with potential for legal liability, compromised ethical behavior and reputation, forcing it to be taken down in 16 hours.

**Disinformation & Reputation**

Social media has its own implications for reputational risks e.g. fake news can cause “irreversible damage” to companies, their reputation and can sink their stock price.
**Traditional Risks Manifest as a result of New Triggers**

Is your organization prepared for the new risks posed by the introduction of disruptive technologies?

<table>
<thead>
<tr>
<th>Reputation Risks</th>
<th>Change Risks</th>
<th>Auditability Risks</th>
<th>Compliance Risks</th>
<th>Security &amp; Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Inconsistency across technology platforms</td>
<td>✓ New business models and workflows</td>
<td>✓ Integrity of record keeping</td>
<td>✓ Ensuring compliance during rapid change</td>
<td>✓ More access points and devices holding data</td>
</tr>
<tr>
<td>✓ Unapproved use of third-party technology platforms</td>
<td>✓ Change to Agile methods</td>
<td>✓ Integrity of transaction processing</td>
<td>✓ Redundancy of experts post automation</td>
<td>✓ Aggregation of sensitive data</td>
</tr>
<tr>
<td>✓ Overall increase in complexity with exposure to multiple 4th and 5th party code and technology</td>
<td>✓ Pace of change exceeds capacity</td>
<td>✓ Integrity of digital business processes</td>
<td>✓ Evolving testing paradigms to keep pace with rapid change</td>
<td>✓ More data in easily accessible form</td>
</tr>
<tr>
<td></td>
<td>✓ Disruption of existing cash flow</td>
<td>✓ Maintaining the auditability of data within digital frameworks and extended enterprise</td>
<td></td>
<td>✓ Increased sophistication of cyber threats</td>
</tr>
<tr>
<td></td>
<td>✓ Talent gaps to manage digital assets</td>
<td></td>
<td></td>
<td>✓ Higher volume and multi-point customer data collection</td>
</tr>
</tbody>
</table>
What is the most challenging aspect of auditing disruptive technologies?

1. Lack of knowledge of risks
2. Hard to figure when to get involved
3. They are embedded inside other solutions
4. All the above
The Digital Risk Management Framework

This structure allows a consistent approach to risk management across disruptive technologies.
## Sample of Risks Introduced by Robotic Process Automation

IA functions will require to prioritize on net new risks introduced by disruptive technologies.

| Technology Deployment Lifecycle | 1. With increased **transaction processing speeds**, processing errors undetected during testing can proliferate fast causing losses or reputation risk. |
| | 2. **Testing complexity** in cases where target systems **do not have equivalent non-production environments**. |
| | 3. **Apps may not respond to bot speeds**; overloading of source applications. |
| | 4. **Complexity in disaster recovery** and business continuity as more processes are automated. |
| Governance | 5. **Governance for new technology assets** (Bot IDs, Bot machines, Automated Processes). |
| | 6. **Change management complexity** due to new systems, automated-process, undocumented configuration items (e.g. document folder structures) with complex interrelationships. |
| | 7. Inadequate communication leading to **fear of job loss and poor employee morale**. |
| | 8. **Unauthorized use of tools** (like Shadow IT) exposing the organization to unintended risks. |
| Business Process | 9. Lack of clarity on **roles and responsibilities** between IT and business causing interim risks. |
| | 10. **Accumulation of privileges** (especially when same bot has multiple roles to manage licenses) can increase the complexity to manage and vulnerability when hacked. |
| | 11. **Automation of a bad process**. Controls designed for people **might not translate** effectively to bots. |
| | 12. **Loss of knowledge workers** made redundant by automation and unavailability when needed. |
Sample of Risks Introduced by Cognitive Intelligence

IA functions will require to prioritize on net new risks introduced by disruptive technologies

1. **Algorithms generate inaccurate results** or are used beyond intended parameters leading to incorrect business decisions.
2. Self-learning AI, or AI that includes a feedback loop, often involves changes being made directly into the production environment.
3. **Complexity in disaster recovery and business continuity** as more processes are centrally automated.
4. The volume of data processes increases the threat of targeting through Cyber crime.
5. Disparate coding standards for developing algorithm’s can lead to long-term support issues.
6. Feedback into AI models is poorly controlled leading to inaccuracies in the model and output.
7. Automation of a bad process may delay or override the much needed addressing of underlying root causes and redesigning poor processes or upgrading systems.
8. Algorithms developed and trained on data sets that deliberately or inadvertently create bias or ethical issues.
9. Human involvement may be able to identify issues that are not apparent to the bot.
10. **Accumulation of privileges** (especially when same bot has multiple roles to manage licenses) can increase the complexity to manage and vulnerability when hacked.
11. With increased transaction processing speeds, processing errors undetected during testing can proliferate fast causing losses or reputation risk.
Sample of Risks Introduced by Blockchain
IA functions will require to prioritize on net new risks introduced by disruptive technologies

<table>
<thead>
<tr>
<th>Technology Deployment Lifecycle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. While blockchain technology provides transaction security, it <strong>does not guarantee account/wallet security</strong>.</td>
</tr>
<tr>
<td>2. Additional technology concerns could <strong>include speed, scalability, and interface with legacy systems</strong> in implementing blockchain technology.</td>
</tr>
<tr>
<td>3. <strong>Smart contracts</strong> may be susceptible to <strong>security breaches and improper administration.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Currently, in many geographies, there is <strong>uncertainty around the regulatory requirements</strong> related to blockchain applications, which also includes <strong>cross-board regulations related to privacy and data protection.</strong></td>
</tr>
<tr>
<td>5. <strong>Legal liability remains unclear</strong> for an improper, erroneous, or a malicious administration of a smart contract resulting in a transaction with two or more entities on the network, causing assets to leave the network via those transacting entities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Digital assets could become irretrievable in the case of <strong>accidental loss or theft of private keys</strong>, especially given the lack of a single controller or a potential escalation point.</td>
</tr>
<tr>
<td>7. Adoption of blockchain may introduce <strong>new liquidity risk</strong> as there may not be intermediaries to take on the counterparty risks.</td>
</tr>
<tr>
<td>8. <strong>Consensus protocols</strong> should be evaluated in the context of the framework, the use case, and network participant requirements to ensure <strong>integrity of transactions.</strong></td>
</tr>
</tbody>
</table>
Poll Question #3

Do disruptive technologies truly introduce net new risks?

1. Yes
2. No
3. Unsure
Balance between assurance and advisory
Go beyond controls and compliance by offering actionable insights to build resilience and create value

Assure

Testing
Access to documentation of testing procedures and independently review testing performed by sampling test cases documented, results generated and issues logged.

Exception Handling and Monitoring
Monitor the bots in testing and production environments, as well as triage issues that may arise.

Recertification Process
Encourage business and technology stakeholders to perform an annual recertification of the design and implementation of RPA and CI smart automation technologies.

Advise

Process Documentation
Encourage the creation and maintenance of pre-implementation documentation that can be easily audited.

Disseminate Changes in Risk Assessment Process
Adapt a continuous risk assessment process to be able to evaluate innovation impact on timely basis integrating technological changes.

Execute Dynamic Audit Procedures
Execute dynamic and effective audits more frequently and perform audits using an agile framework.

Updates to Reporting
Identify the level and structure of reporting required for RPA and CI automation audits.
# Role of Internal Audit Across the Disruptive Technology Development Lifecycle

Audit transformation through innovation and technology

<table>
<thead>
<tr>
<th>Ideation</th>
<th>Design</th>
<th>Development</th>
<th>Validation</th>
<th>Implementation &amp; Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Line of Defense: Management</td>
<td>• Conduct Market and Technical research</td>
<td>• Develop a Vision, Assess Feasibility and risk alignment</td>
<td>• Create back-end solution to support the front-end design</td>
<td>• Test, test and deploy</td>
</tr>
<tr>
<td>2nd Line of Defense: Risk Mgmt. &amp; Compliance Functions</td>
<td>• Analyze business needs</td>
<td>• Identify and evaluate front-end design alternatives</td>
<td>• Produce a Model or Prototype and Test</td>
<td>• Gather post-launch analytics</td>
</tr>
<tr>
<td>3rd Line of Defense: Internal Audit</td>
<td>• Brainstorm and select ideas</td>
<td>• Brainstorm and select ideas</td>
<td>• Identify and evaluate front-end design alternatives</td>
<td>• Closely monitor bugs or defects missed in testing</td>
</tr>
</tbody>
</table>

**Ideation**
- Understand the selected initiative and assess extent of involvement
- Identify any emerging issues that may require special attention

**Design**
- Perform/Review initial risk assessment and define the target risk exposure
- Provide risk management frameworks and any clarifications thereof

**Development**
- Review and Challenge controls developed by first line
- Assess adherence to standards for secure and continuous access to key sources of business data

**Validation**
- Challenge management’s plan to:
  - Monitor the adequacy and effectiveness of the implementation
  - Monitor the compliance with applicable laws and regulations

**Implementation & Monitoring**
- Challenge management’s plan to:
  - Provide guidance and training
  - Managing changes
  - Monitoring incidents

**1st Line of Defense: Management**
- Understand the selected initiative and assess extent of involvement
- Understand role played by second line
- Plan involvement in committees or Sprints

**2nd Line of Defense: Risk Mgmt. & Compliance Functions**
- Understand the selected initiative and assess extent of involvement
- Understand role played by second line
- Plan involvement in committees or Sprints

**3rd Line of Defense: Internal Audit**
- Concerns:
  - Adequacy of work done by second line
  - Adequacy of actions to address second line findings

© Deloitte LLP and affiliated entities.
## Embedding Digital Throughout the Internal Audit Lifecycle

**Building resilience in internal audit during COVID-19**

### Key Activities

<table>
<thead>
<tr>
<th>Risk Assessment</th>
<th>Audit Planning</th>
<th>Design Effectiveness Assessment</th>
<th>Fieldwork</th>
<th>Reporting / Closing</th>
<th>Issue Tracking / Ongoing Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establish the audit entity universe</td>
<td>• Communicate intention to audit</td>
<td>• Perform detailed audit planning</td>
<td>• Hold opening meeting</td>
<td>• Produce audit report overview</td>
<td>• Utilize history of issues tracking to develop insights through trends analysis and KPIs</td>
</tr>
<tr>
<td>• Assess completeness of audit universe</td>
<td>• Conduct introduction/scoping meeting</td>
<td>• Develop testing strategy</td>
<td>• Create Operating Effectiveness Testing work papers and execute testing in accordance with the audit strategy</td>
<td>• Issues in the report</td>
<td>• Establish continuous auditing</td>
</tr>
<tr>
<td>• Analyze risk profile of the audit entity</td>
<td>• Complete Audit Planning Memorandum (APM)</td>
<td>• Review and approve Design Effectiveness Assessment</td>
<td>• Evaluate operating effectiveness of key controls</td>
<td>• Conduct overall assessment</td>
<td>• IA Compliance Risk Assessment</td>
</tr>
<tr>
<td>• Identify audit needs and develop audit plan</td>
<td>• Develop process understanding</td>
<td>• Draft issues</td>
<td>• Draft audit report</td>
<td>• Draft audit report</td>
<td>• Location risk assessment visualization</td>
</tr>
<tr>
<td>• Conduct business monitoring</td>
<td>• Identify inherent risks and key controls</td>
<td></td>
<td>• Issue Final audit report</td>
<td>• Issue Final audit report</td>
<td>• Cross business unit/region comparative and flux analysis</td>
</tr>
<tr>
<td></td>
<td>• Complete risk control matrix</td>
<td></td>
<td>• Perform audit folder closure</td>
<td>• Perform audit folder closure</td>
<td>• Continuous business operations monitoring</td>
</tr>
<tr>
<td></td>
<td>• Complete Audit Announcement Memo</td>
<td></td>
<td>• Analyze audit budget vs actual</td>
<td>• Conduct audit team de-brief</td>
<td>• Risk assessment dashboard</td>
</tr>
</tbody>
</table>

### Representative Tasks

<table>
<thead>
<tr>
<th>Tech</th>
<th>Risk Assessment</th>
<th>Audit Planning</th>
<th>Design Effectiveness Assessment</th>
<th>Fieldwork</th>
<th>Reporting / Closing</th>
<th>Issue Tracking / Ongoing Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Automation of text-heavy documents</td>
<td>• IA Compliance Risk Assessment</td>
<td>• Automation of text-heavy documents</td>
<td>• Population testing</td>
<td>• Automated generation of text-based audit reports</td>
<td>• Real-time reporting of frauds arising in financial systems</td>
<td></td>
</tr>
<tr>
<td>• Profile business operations</td>
<td>• Location risk assessment visualization</td>
<td>• Data modelling and batched reporting</td>
<td>• Data aggregation and integration</td>
<td>• Data visualization / audit story board</td>
<td>• Enhanced dash-boarding and reporting</td>
<td></td>
</tr>
<tr>
<td>• Exploratory analytics and ‘what-if’ analysis</td>
<td>• Cross business unit/region comparative and flux analysis</td>
<td></td>
<td>• Intelligent detection of suspicious logs associated with IT systems</td>
<td>• Impact quantification</td>
<td>• Thematic risk identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Continuous business operations monitoring</td>
<td></td>
<td></td>
<td></td>
<td>• Chief Audit Executive dashboard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Risk assessment dashboard</td>
<td></td>
<td></td>
<td></td>
<td>• Issue tracking visualization</td>
<td></td>
</tr>
</tbody>
</table>
Role of Internal Audit Across the Disruptive Technology (DT) Development Lifecycle

Audit transformation through innovation and technology

1. Balance between pushing the frontiers and risk appetite
   - Have a seat at the table when strategic decisions are made on DT, including around governance.
   - Proactively understand the DT journey undertaken by business units.
   - Evaluate the impact of the DT on the organization, processes, controls, resources, geography, regulatory landscape, cyber and third-party oversight and share insights.

2. Prepare to be strategically relevant focusing on: Talent. Tools. Techniques
   - Determine required DT skillsets for Internal Auditors and deploy training.
   - Understand net new risks introduced by various disruptive Technologies and consider the impact on current audit programs.
   - Identify new tools and capabilities required to conduct effective audits (e.g. Data analytics, Predictive Project Analytics, Security).

3. Execute agile/dynamic audit procedures
   - Understand the DT journey risks and impact on Business Processes and assess design of controls and their operating effectiveness post go-live.
   - Assess controls over risks caused by disruptive tech: Agile, AI, Automation, Blockchain, Cloud, Data Analytics etc.
   - Understand governance structure and their effectiveness to offer oversight.

4. Consider updates to reporting
   - Identify level and structure of reporting that will be conducted:
     - Technology level vs. business function level
     - Assurance-driven vs. consultative
     - Frequency and speed of audits

© Deloitte LLP and affiliated entities.

Auditing disruptive technologies – IIA Edmonton Chapter
Thank You.

Q & A

Baskaran Rajamani
Email: brajamani@deloitte.ca

Mark Varma
Email: mvarma@deloitte.ca