BUILDING THE INTERNAL AUDIT FUNCTION OF THE FUTURE

IIA CHICAGO CHAPTER 59TH ANNUAL SEMINAR 2019
Emerging Technology Risks and Intelligent Automation Considerations for the Internal Auditor (from RPA and Beyond)

Kelly Combs, KPMG Director, Emerging Technology Risk
Clinton Peters, KPMG Director, Internal Audit & Enterprise Risk
April 1, 2019
Clinton Peters, CPA, CIA, CFE  
KPMG LLP, Director, Advisory Consulting, Internal Audit and Enterprise Risk

Clinton is a Director of KPMG’s Chicago-based Internal Audit & Enterprise Risk (IA&ER) services practice with more than 15 years of public accounting and professional services experience. Clinton is adept at process reengineering and has gained extensive experience leading, managing and executing internal audit programs, internal control over financial reporting (ICOFR) programs, Sarbanes-Oxley 404 (SOX) compliance programs, and other risk management programs across a variety of industries. Clinton has also successfully developed and implemented internal audit and ICOFR functions for several leading national and global organizations.

As KPMG’s designated Intelligent Automation Network Champion for the Midwest, Clinton is responsible for promoting awareness of intelligent automation, educating clients and KPMG professionals on the automation considerations for internal audit.

Kelly Combs  
KPMG LLP, Director, Advisory Consulting, Emerging Technology Risk Services

Kelly is a Director in KPMG’s Emerging Technology Risk practice with experience in Robotic Process Automation (RPA) and Intelligent Automation platforms. She has led and executed engagements across a range of industries and sectors including Technology, Media and Telecommunications, Manufacturing, Consumer Markets, and Healthcare. Kelly has also delivered a wide range of traditional and innovative solutions to her clients including emerging technologies (i.e., mobile, cloud, Intelligent Automation) risk assessments, technology enabled business process reviews and controls integration, IT audit support for Sarbanes Oxley and Financial Statement Audits, IT Internal Audit projects over emerging technologies, Service Organization Control (SOC) reporting, and various other risk and compliance related engagements. In addition, Kelly has experience with medium-large sized clients with complex IT environments (40+ systems).
Learning Objectives

At the conclusion of today’s seminar, participants will walk away with an awareness of:

- Recent technology advancements and their potential uses
- The automation continuum, as well as the classes of automation technologies that span this continuum
- The various ways in which recent technology advancements (including automation) have changed, and will continue to change, how business is done
- How recent technology advancements (including automation) are impacting the Three Lines of Defense, including Internal Audit
- Important governance, risk and control considerations
Emerging technology radar
Emerging technology radar

- Artificial intelligence
- Digital platforms
- Immersive experience, AI & Digital platforms
- Impact
- Transformational
- High
- Moderate

Key Technologies:
- Quantum computing
- Artificial General Intelligence
- Augmented reality
- Machine learning
- Drones
- Conversational user interfaces
- Augmented Data Discovery
- Smart robots
- Virtual reality
- Edge computing
- Virtual assistants
- Software defined security
- Digital twin
- Cognitive computing
- Augmented reality
- Virtual reality
- Connected home
- Cognitive expert advisors
- IoT platform
- Neuromorphic hardware
- Brain Computer Interface
- Virtual reality
- Smart robots
- Nano tube electronics
- 4D printing
- Nanotube electronics
- Market entry
- Strategic technologies
- Blockchain
- 3D printing
- Serverless PaaS
- 5G
- Edge computing
- Visionary experience
- Artificial intelligence
- Digital platforms
- Impact
- Transformational
- High
- Moderate
Cognitive technology and RPA

Cognitive systems are an application of interpreting and learning systems and redefine the relationship between human and machine.

$152B+
The expected market size for digital labor by 2020*

ROI between 600 – 800%*

45% of activities individuals currently perform in the workplace can be automated using existing technologies*

* Bank of America Merrill Lynch, November 2015
* London School of Economics, The IT Function and Robotic Process Automation, October 2015
The “4th industrial revolution” (cyber-physical systems) is beginning and its impact is profound according to the World Economic Forum founder, Klaus Schwab.
The spectrum of automation technologies

**Rules**
- Basic process automation
  - Macro-based applets
  - Screen level and OCR data collection
  - Workflow automation
  - Process mapping
  - Self executing

**Learn**
- Enhanced automation
  - Built-in knowledge repository
  - Learning capabilities
  - Ability to work with unstructured data
  - Pattern recognition
  - Reading source data manuals
  - Natural language processing

**Reason**
- Cognitive automation
  - Artificial intelligence
  - Natural language recognition and processing
  - Self-learning (sometimes self optimizing)
  - Processing of super data sets
  - Predictive analytics/hypothesis generation
  - Evidence-based learning

**Think like a human**
Definitions – AI ≠ RPA

Artificial Intelligence
We refer to ‘AI’ as technology capable of performing tasks commonly associated with intelligent beings. AI typically includes four elements: sensing, learning, inference and reasoning. Generally, when we refer to ‘AI’ in the context of ‘AI In Control’ we refer to Machine Learning models.

Robotic Process Automation
We use the term Robotics (RPA) to refer to advanced automation of tasks, previously carried out by humans, through hard coded/configured software. The process often remains the same unless humans change the code, with the system unable to cope with undefined scenarios.

Note: We expect that this distinction will disappear over time, as ‘intelligence’ will become increasingly integrated into technology solutions.

Source for definitions in the area of AI: https://home.kpmg.com/content/dam/kpmg/uk/pdf/2018/06/trust_in_artificial_intelligence.pdf
**Illustrative AI use cases across all sectors**

<table>
<thead>
<tr>
<th>Sector</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking &amp; Insurance</td>
<td>* Algorithms to predict/identify potential misuse of credit cards.</td>
</tr>
<tr>
<td></td>
<td>* Algorithmic high-frequency trading.</td>
</tr>
<tr>
<td>Energy, Natural Resources &amp; Chemicals</td>
<td>* Smart grid algorithms to optimally distribute energy supply.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to determine optimal production capacity per machine.</td>
</tr>
<tr>
<td>Automotive</td>
<td>* Algorithms for autonomous vehicles.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms for engine control and optimal energy distribution.</td>
</tr>
<tr>
<td>Public sector</td>
<td>* Algorithms to allocate children to schools.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms for predictive policing.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to assess the risk of child abuse and neglect through statistical modeling.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to perform making legal decisions.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to detect Tax fraud.</td>
</tr>
<tr>
<td>Industrial Manufacturing</td>
<td>* Algorithms to improve demand forecast accuracy and to reduce energy costs and negative price variances.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to predict maintenance.</td>
</tr>
<tr>
<td>Transportation &amp; Leisure</td>
<td>* Algorithms to predict and detect traffic accidents and conditions by converting traffic sensors into 'intelligent' agents using cameras.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to automatically manage train timetables.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to perform Yield management.</td>
</tr>
<tr>
<td>Life sciences</td>
<td>* Algorithms to advise whether to build a new road, how much money should be allocated to maintenance and rehabilitation activities and which road segments or bridges to maintain and whether to divert traffic to an alternative route in an incident situation.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to predict epidemic outbreaks.</td>
</tr>
<tr>
<td>Professional &amp; Business services</td>
<td>* Algorithm based sorting of resumes and job applications.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to replaceaccountancy services and automatically perform audit procedures.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to automatically perform due-diligence services.</td>
</tr>
<tr>
<td>Retail</td>
<td>* Algorithms to define consumer profiles and optimize marketing spendings.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to automatically test and predict behavior of combinations of ingredients (both for food as well as for instance personal care products).</td>
</tr>
<tr>
<td>Media &amp; Telecommunications</td>
<td>* Algorithms to assign news articles to users.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to detect fake news.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to detect idle channels and allocate them efficiently.</td>
</tr>
<tr>
<td>Technology</td>
<td>* Search engine algorithms.</td>
</tr>
<tr>
<td></td>
<td>* Robotics.</td>
</tr>
<tr>
<td></td>
<td>* Automatic face recognition for different purposes.</td>
</tr>
<tr>
<td>Healthcare</td>
<td>* Computerized health diagnostics algorithms.</td>
</tr>
<tr>
<td></td>
<td>* Predictive hospitalization algorithms.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to prevent medical errors and reduce hospital readmission.</td>
</tr>
<tr>
<td>Consumer Goods, Food &amp; Drink</td>
<td>* Algorithms to analyze market demand curve of a product.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to understand and predict the demand curve of a product.</td>
</tr>
<tr>
<td>Energy, Natural Resources &amp; Chemicals</td>
<td>* Smart grid algorithms to optimally distribute energy supply.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to determine optimal production capacity per machine.</td>
</tr>
<tr>
<td>Media &amp; Telecommunications</td>
<td>* Algorithms to assign news articles to users.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to detect fake news.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to detect idle channels and allocate them efficiently.</td>
</tr>
<tr>
<td>Technology</td>
<td>* Search engine algorithms.</td>
</tr>
<tr>
<td></td>
<td>* Robotics.</td>
</tr>
<tr>
<td></td>
<td>* Automatic face recognition for different purposes.</td>
</tr>
<tr>
<td>Technology</td>
<td>* Computerized health diagnostics algorithms.</td>
</tr>
<tr>
<td></td>
<td>* Predictive hospitalization algorithms.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms to prevent medical errors and reduce hospital readmission.</td>
</tr>
<tr>
<td>Technology</td>
<td>* Search engine algorithms.</td>
</tr>
<tr>
<td></td>
<td>* Robotics.</td>
</tr>
<tr>
<td></td>
<td>* Automatic face recognition for different purposes.</td>
</tr>
<tr>
<td>Logistic</td>
<td>* Algorithms for autonomous trucks.</td>
</tr>
<tr>
<td></td>
<td>* Algorithms for automated vehicle routing.</td>
</tr>
</tbody>
</table>
Governance, Risk, and Control Considerations
Real world examples of where AI went bad

- Target Figures Out Teen is Pregnant – Before She’s Told Anyone
- Nude Webcams & Facebook Ads Teens Weren’t Supposed to See
- Twitter teaches Microsoft’s AI chatbot to be a racist in less than a day
- AMAZON SCRAPS ‘SEXIST AI’ RECRUITMENT TOOL
- Chinese billionaire’s face falsely identified by law enforcement from an bus advertisement
- Uber self-driving car kills a pedestrian
- Facebook chatbots shut down after developing their own language
- Facebook chatbots shut down after developing their own language
Amazon scraps ‘sexist AI' recruitment tool

**Goal** – To create a tool which identified the most talented candidates based on their CV and application information, giving the recruiter the top 5 candidates from hundreds of applications.

**Approach** – Create a supervised machine learning model, based off historic applications and details of which applicants were hired.

**What went wrong?** Very quickly it became apparent the ML model was almost exclusively selecting men for roles. There was a big public outcry and Amazons reputation was damaged and significant development costs lost as they were forced to terminate the project to limit reputational damage.
### Risks: Machine learning vs. RPA

<table>
<thead>
<tr>
<th>Machine learning</th>
<th>RPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lack of accountability</strong> for actions performed</td>
<td>Lack of accountability for actions performed</td>
</tr>
<tr>
<td>Use of <strong>disallowed data sources</strong> e.g. protected groups</td>
<td>Only uses the data categories specified in the configuration</td>
</tr>
<tr>
<td>Trained from <strong>Bias/misrepresented Data</strong></td>
<td>Structured around inefficient processes</td>
</tr>
<tr>
<td>Can divine its <strong>own best path</strong> to achieve the outcomes</td>
<td>Only as good as the human implementing it</td>
</tr>
<tr>
<td><strong>Black box</strong> lacking explainability</td>
<td>No issues around explainability</td>
</tr>
<tr>
<td><strong>Model functionality drift</strong></td>
<td>Static process which wont evolve without human interference</td>
</tr>
<tr>
<td>Malicious data inputs from external sources (<strong>Adversarial Attack</strong>)</td>
<td>Process followed is fixed and cant be manipulated by malicious data inputs</td>
</tr>
</tbody>
</table>
Importance of AI governance

Below we see most company’s use or plan to use AI, but a large majority lack confidence in the governance and are unsure how to audit AI.

Believe AI is either already being used or is planned for: 97%
Lacked confidence in AI governance in place: 80%
Planned to perform an audit on their AI solutions: 45%
Lacked a clear approach to audit AI: 70%

Survey from 170 technology risk professionals at IT IA conference in November 2018
Other common risks and pitfalls of intelligent automation programs

As organizations implement intelligent automation programs, there are common pitfalls related to the emerging governance, risk, and control considerations related to such programs.

Understanding these potential pitfalls—and why they matter to the success of the program and organization—can help the organization develop a plan to mitigate, or even prevent, such issues.

- Undefined ownership of intelligent automation program
- General lack of oversight of risk
- General lack of program oversight
- Lack of consistent and secure development and management of bots.

- Varying skill levels and inconsistent developer training
- Lack automated alerting tools for error handling and resolution
- General lack of controls around “is the bot doing what it is supposed to be doing”

- Key automation risks:
  - Inadvertent risk acceptance and reliance produces unexpected negative results
  - Accountability, segregation of duties, and compliance issues
  - Unnoticed control failures impacting processing and compliance
  - Ineffective design of controls

- Lack controls for proper ownership of Bot ID and effective integration of the Bot IDs with applications.
- Lack of bot accountability relating to security, privacy, and compliance requirements.
- Improper bot access provisioning and password management.
- Lack of formal process for assessing how source application changes affect Bots that access them.
- Lack formal and consistent process for requesting and implementing changes to Bots.
- Lack of segregation of RPA development and production.
Governance, risk, and control considerations for the intelligent automation lifecycle

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>◦ Ownership and accountability of bots</td>
<td>◦ Understanding the nature of the data the bots access and their interaction with applications</td>
<td>◦ Business continuity and disaster recovery</td>
</tr>
<tr>
<td>◦ Identification of impacted regulatory requirements and privacy considerations</td>
<td>◦ Helping ensure bots are developed to specified requirements and secure coding practices and tested</td>
<td>◦ Monitoring and error handling</td>
</tr>
<tr>
<td>◦ Risk and governance committees</td>
<td>◦ Principles of “least privilege” for logical access/layered security model</td>
<td>◦ Auditing, logging, and traceability</td>
</tr>
<tr>
<td>◦ Organizational and people change management</td>
<td>◦ Secured authentication and encrypted communication channels</td>
<td>◦ Processing integrity</td>
</tr>
<tr>
<td>◦ Program management</td>
<td>◦ Skills, capabilities, and training</td>
<td>◦ Skills, capabilities, and training</td>
</tr>
<tr>
<td></td>
<td>◦ Vendor risk management</td>
<td></td>
</tr>
</tbody>
</table>
How to Assess and evaluate AI
# Challenges and benefits of auditing AI

<table>
<thead>
<tr>
<th>Challenges for the auditor of AI</th>
<th>Keys to the successful auditing of AI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Immature auditing frameworks or regulations specific to AI</td>
<td>1. Adopt and adapt existing frameworks and regulations.</td>
</tr>
<tr>
<td>2. Limited precedents for AI use cases</td>
<td>2. Explain and communicate proactively about AI with stakeholders.</td>
</tr>
<tr>
<td>3. Uncertain definitions and taxonomies of AI</td>
<td>3. Explain and communicate proactively about AI with stakeholders.</td>
</tr>
<tr>
<td>5. Emerging nature of AI technology</td>
<td>5. Become informed about AI design and architecture to set proper scope.</td>
</tr>
<tr>
<td>7. Lack of strategic starting points</td>
<td>7. Involve all stakeholders.</td>
</tr>
<tr>
<td>8. Possibly steep learning curve for the AI auditor</td>
<td>8. Become informed about AI design and engage specialists as needed.</td>
</tr>
</tbody>
</table>

* Take from ‘Auditing Artificial Intelligence’ - ISACA
Three approaches to achieve trust

For AI to be deployed successfully, organizations and society need to be able to trust it to make the right decisions and/or not to make the wrong decisions. A comprehensive framework includes three approaches to achieving trust in AI solutions.

01 Comparing outcomes to another source(s)
- Another (reliable) source might not exist
- Not always feasible to replicate the model/develop an alternative
- And if you have another source: why develop the AI solution in the first place?

02 Understand and validate the AI model(s)
- Model might be too complicated for humans to understand
- Model uses techniques such as deep neural networks that are notorious in terms of explainability.

03 Develop AI solution(s) in a controlled environment
- Skilled people using a rigorous methodology in a secure environment is no guarantee for quality outcomes
- Using a rigorous methodology is in tension with an agile and explorative approach that is common in data science.

A comprehensive governance framework helps define the optimal combination of controls across these three approaches.
Key Pillars to Trust in AI

**Integrity**
Track the lineage and provenance of raw data, training data, model experiments, ongoing changes made by SME’s. Model training incl changes by stored in a immutable ledgers.

**Free from Bias**
Models as well as the training data that must be free of bias, are inclusive and avoids unfair treatment of certain protected groups. Be certain that the models incl the trainer comply with policies & regulations.

**Explainability**
Models that can explain the knowledge learned. Can provide explanation in business terms on how decisions were made. Interpretations are gained or inferred from explanations.

**Agile and robust**
Models are interoperable between various runtimes, providers, or frameworks. Consumable from apps & processes. The models, ground truth and feedback are safe and secure from harm or adversarial attacks.
Automation and the Evolution of Internal Audit
Automation is changing the role, activities, and skillsets required from Internal Audit

As businesses embrace the use of intelligent automation across their operations, internal audit functions will come under increasing pressure to also change.

The roles and activities that internal audit functions perform today might not be relevant in the future as organizations transform increasingly complex business activities leveraging intelligent and other technology solutions. Few internal audit functions today are positioned for the task of providing assurance over the complex and data-rich operating environments expected to become more prevalent in the years ahead.

Only 13% of chief audit executives strongly agree that their internal audit functions are quick to adopt new technologies or processes, while just 32% strongly agree that their internal audit functions challenge their own status quos.
In a business environment that’s changing at a faster rate than ever before, internal auditors play an increasingly important role.

With the vast uncertainties presented by an onslaught of disruptive forces, the internal audit function must keep pace to help the organization understand and manage the associated risks, achieve expected results from automation, and continue to innovate to add value.

Internal Audit can help identify opportunities to automate inefficient business processes, including opportunities to embed automation-enabled control activities throughout the organization.

Internal Audit can help to integrate governance, risk, and controls considerations into the governance framework of the automation program lifecycle, as an organization establishes and implements its intelligent automation program.

Finally, Internal Audit can leverage intelligent automation to transform internal audit, increasing the efficiency and effectiveness of its own activities.
Automation Opportunities Brought to Life
Opportunities to automate the 1st and 2nd Lines: Automating Control Activities

As businesses embrace the use of intelligent automation across their operations, Internal audit functions need to stay informed of these changes, at the on-set and throughout, so they can advise management of opportunities to embed automation-enabled control activities.

Some examples of areas where automated solutions for controls include:

### Automation of business process controls
- **Manual**
  - Reconciliations
  - Accounts receivable aging
  - Cash transfers
  - Journal entry analysis
  - Fee calcs
  - Loan review
  - Nightly settlement
  - Contract compliance

- **Automated**
  - Edit checks
  - Validations
  - Calculations
  - Interfaces
  - Reports

- **Other controls**
  - Compliance
  - Cyber security
  - Payments
  - Regulatory compliance
  - Payments reconciliations
  - Positive pay validation

### Automation of IT controls
- **Change management**
  - Changes are authorized
  - Changes are tested
  - Changes are approved
  - Developer access to production

- **Logical access**
  - Passwords
  - New users
  - Periodic review
  - Terminations
  - Segregation of duties

- **Computer operations**
  - Incident management
  - Backups
  - Job scheduling
  - Physical security
Case study – User access review

**Challenge**
The organization had grown rapidly through acquisitions resulting in around 30+ systems in scope for compliance. As a result, the manual effort to perform their quarterly User Access Review (UAR) was enormous. Reviews were either being partially complete, or were not being started at all.

**KPMG’s Response**
Through review of the existing process and discussions with the client, KPMG identified the following challenges:

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieving complete and accurate user data from 30 systems</td>
<td>Configured direct connections to each system to query data on demand.</td>
</tr>
<tr>
<td>Matching legacy user IDs to current HR records</td>
<td>Built a series of pattern based and fuzzy matches to identify an employee's HR record to bring in reviewer assignments and employment status.</td>
</tr>
<tr>
<td>Reviewers unfamiliar with capabilities of each access role</td>
<td>Leveraged data from the company's segregation of duties control to define business process capabilities for access roles.</td>
</tr>
<tr>
<td>Send out thousands of notification and follow-up emails to end users</td>
<td>Developed an email automation to send customized emails for each reviewer with hyperlink to their UAR reports.</td>
</tr>
<tr>
<td>Tracking completion of UAR reports</td>
<td>Developed an automation to review all UAR reports and report on attributes like incomplete reviews and overall completion percentage.</td>
</tr>
</tbody>
</table>

**Results**
Within the first year of the new control operating, 100% of the 4,500 access reviews were completed.
Illustrative process flow

HR Employees

SOD Access Mapping

Application Database

Uploaded Reports to Network Drive

Alteryx Workflows Configured Locally

Email Notification Sent When Report are Ready

Alteryx Server Runs Workflow w/Data from Network Drive and DBs

UAR Report for Each Approver

Reports Written Directly from Alteryx to SharePoint
Challenges & lessons learned

- Lack of clear understanding and documentation on how a system’s access and permissions function
- Frequent changing business requirements to align to company culture and minimize impact on business
- Insufficient time to perform adequate testing procedures
- Data integrity create numerous challenges, such as matching users to their HR record or lack of unique identifier
- Reviewers unfamiliar with a new process
- Normalizing data across systems
Questions and Answers?

END OF PRESENTATION
Thank you for your time and attention!

IIA CHAPTER CHICAGO | 59TH ANNUAL SEMINAR