Emerging & disruptive technology risks

Shawn W. Lafferty, KPMG Partner

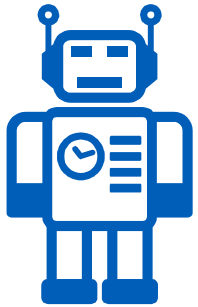
IT Internal Audit/Risk Assurance

–

April 2018

Why IT internal audit?

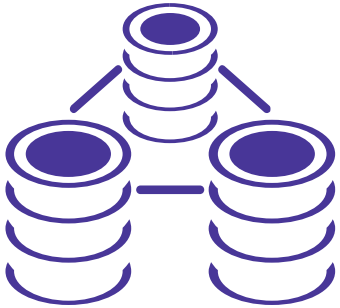
Every day, IT becomes **more complex** and is **changing more rapidly.**



We are beginning to see the deployment of **artificial intelligence** systems;

This means entities must **audit based on the increasing risk** they face and …

…find ways to overcome resource and budgetary constraints.



Key messages

A We've experienced technology disruption before

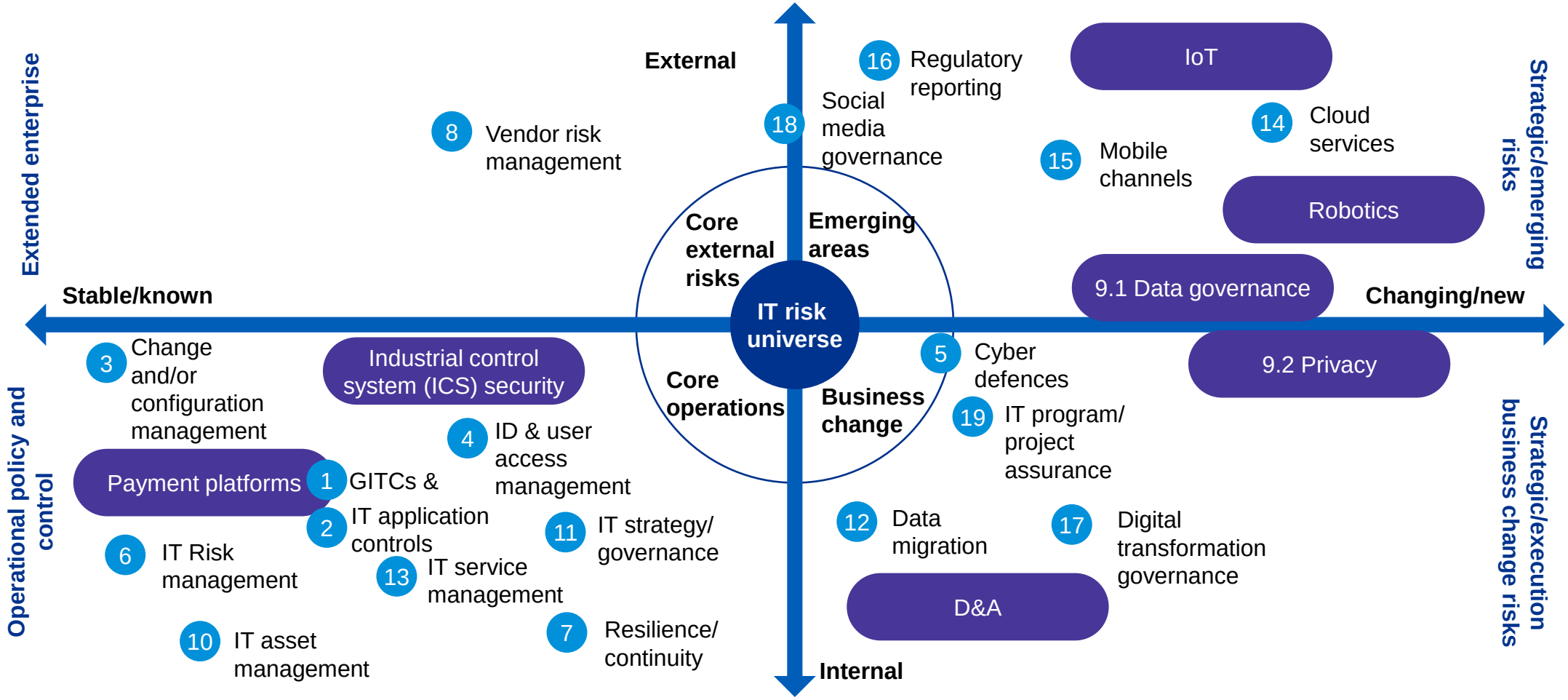
B Audit skills evolve as technology evolves

C Dependency on skilled IT auditors

D Change = Risk

Thinking Forward

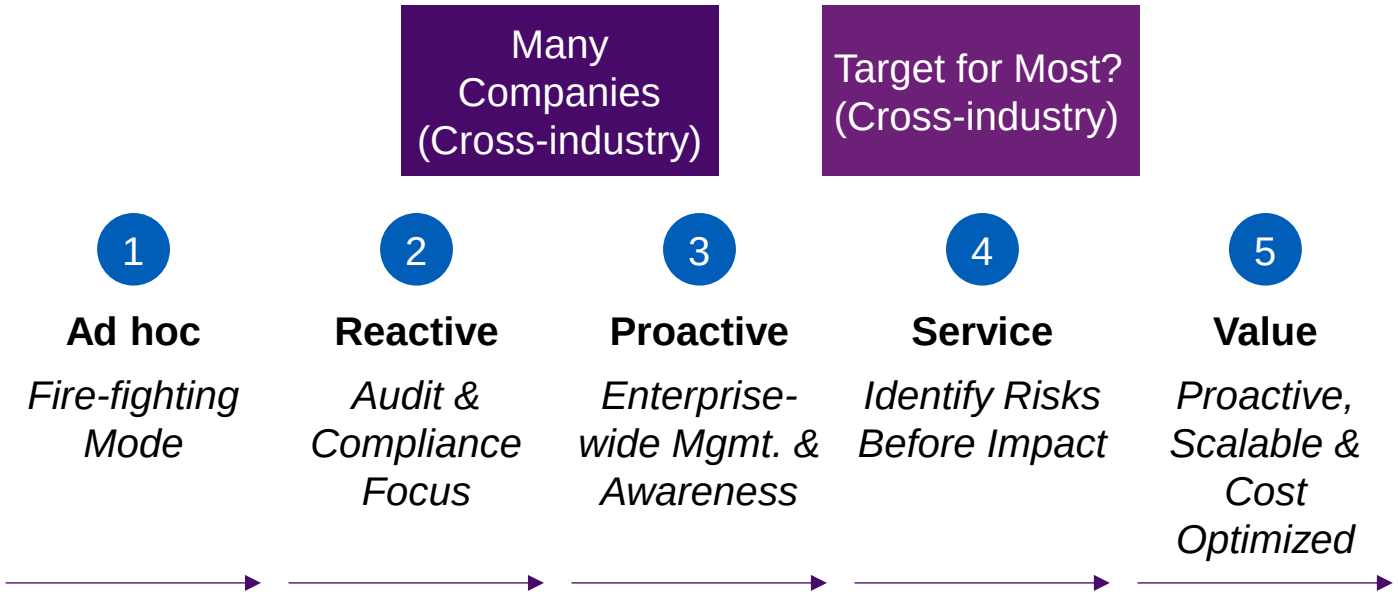
IT internal audit risk universe



Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

Emerging technology risk

There is a shift in focus to **emerging technology risk**, such as artificial intelligence (AI), robotic process automation (RPA) and Internet of Things (IoT). Yet at the same time, organizations cannot afford to neglect the basic areas of risk, including service management areas, access management, industrial control system security and IT disaster recovery.



Source: Managing IT Risk in a Disruptive World, KPMG US, 2017

$

$640,000

Approximate price tag for an IT incident.

4 million

Average number of financial accounts (e.g., credit cards) affected by an IT incident.

776,000

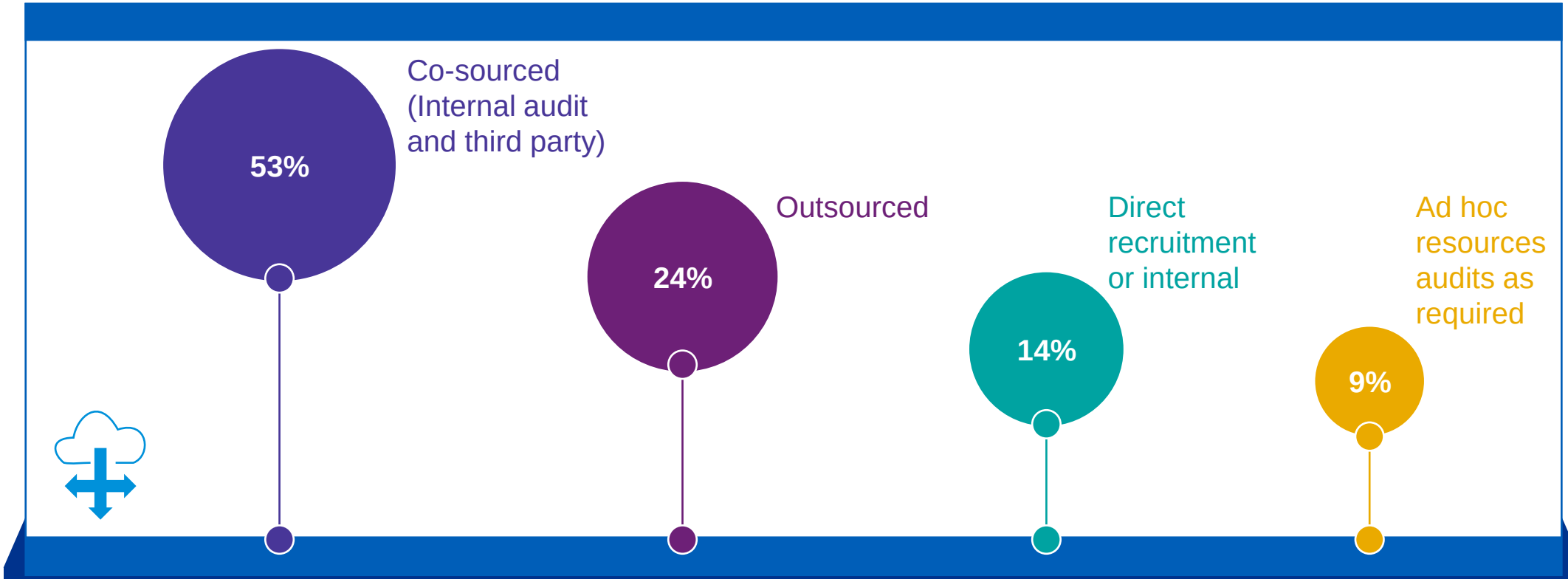
Average number of people (e.g., individuals, patients, employees) affected by an IT incident.

Skill requirements

1. Cyber security
2. D&A
3. Privacy
4. Risk management
5. ERP systems
6. Compliance
7. Change management
8. Software development lifecycle
9. Data quality
10. Independent project assurance
11. Other

Source: IT Internal Audit: Multiplying risks amid scarce resources, KPMG International, 2017

Sourcing skills



What organization has all the skilled ITIA resources it needs; the sheer breadth of skills required and the cost of maintaining, training and developing in-house resources to cover all the risk areas is a very large commitment?

Over three quarters of survey respondents rely on either co-sourced or full out-sourced ITIA delivery models.

AI/RPA is expected to dramatically impact the workplace

$ 152.7 billion

The global market for robots and artificial intelligence is expected to reach $152.7 billion by 2020. The adoption of these technologies could improve productivity by 30 percent.

Bank of America Merrill Lynch

A recent study by HfS Research and KPMG LLP reports that 55 percent of North American enterprises are looking at new opportunities available with RPA systems.

Research from London School of Economics suggests a return on investment in robotic technologies of between 600% and 800% for specific tasks.

600 % and 800 % ROI

MarketsandMarkets estimates that the AI, or cognitive computing marketplace, will generate revenue of

$ 12.5 billion by 2019

$ 14.9 billion

$ 1.7 billion

According to Quid, from 2010 to 2014, private investment in AI grew from $1.7 billion to $14.9 billion, and was on track to grow nearly 50 percent year-on-year in 2015 alone.

Top 5

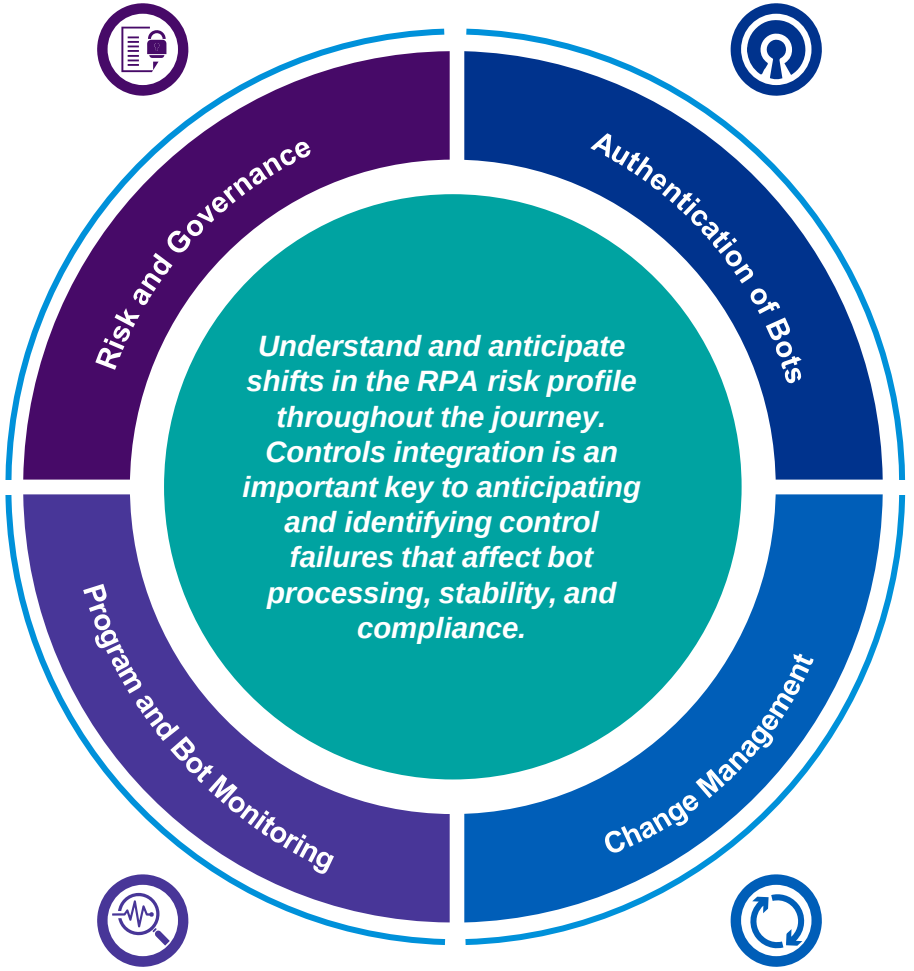
Gartner predicts that by 2020, smart machines will be a top five investment priority for more than 30% of CIOs.

McKinsey research suggests that smart robots will replace more than **100 million knowledge workers** – or one-third of the world's jobs – by 2025.

Key risk considerations in IA/RPA

- Undefined ownership of RPA program among business, IT, Center of Excellence, and/or Supplier
- General lack of oversight of risk mitigation and acceptance process
- General lack of program oversight including KRI and KPI reporting and risk acceptance
- Lack of templates and enablers to help support consistent and secure development and management of bots

- Varying skill levels and inconsistent developer training drives; ineffective logging, monitoring, and analytics capabilities
- Programs often lack automated alerting tools for error handling and resolution and lack trend analysis capabilities
- General lack of controls around “is the bot doing what it is supposed to be doing” (completeness/accuracy/ integrity of data)



- Programs lack controls for proper ownership of bot ID and effective integration of the bot IDs with applications
- Programs often lack design and enforcement of bot ID accountability relating to data elements the bot should have access to in light of security, privacy, and compliance requirements.
- Proper bot access provisioning, password management, and segregation of duties

- There is often a lack of formal process for assessing how source application changes affect bots that access them
- Some RPA programs lack formal and consistent process for requesting and implementing changes to bots
- Segregation of RPA development and production environments is not consistently enforced

Proactively managing risks to enable the journey

RPA programs can present significant risks to the technology control environments. Managing these risks timely and effectively can serve to accelerate innovation, rather than create hurdles.

Plan the bot – typical considerations:

- Bot ownership, accountability, and policies and procedures governing development and operation
- Impacted of regulatory requirements and privacy considerations
- Risk and governance committees
- Organizational and people change management
- Program management

Build the bot – typical considerations:

- Understanding the nature of the data the bots access and their interaction with applications
- Ensure bots are developed to specified requirements and secure coding practices and tested
- Principles of “least privilege” for logical access/layered security model
- Secured authentication and encrypted communication channels
- Skills, capabilities, and training

Manage the bot – typical considerations:

- Business continuity and disaster recovery
- Monitoring and error handling
- Auditing, logging, and traceability
- Processing integrity and data privacy
- Skills, capabilities, and training
- Vendor risk management

Related actions drive company design of related automation, security, and control frameworks that can actually inform and enable the RPA journey.

Embedding and sustaining RPA governance and risk management practices

Plan	Build	Manage	Improve
Understand risk profile and appetite including business and compliance requirements that will inform the RPA governance program	Launch governance and integrate controls, policies, procedures, training, templates, and accelerators for consistent and effective risk management	Embed into day-to-day operations, monitoring performance and effectiveness; continuously identify, monitor, and manage risks	Identify and advocate for opportunities to improve across RPA solutions in the current and target state
— Understand risk profile and tolerance based on organizational, functional, industry, and regulatory landscape, as well as compliance requirements — Evaluate use cases, solution platform(s), strategy, and road map for alignment with risk profile and tolerance	— Enable risk management in the delivery of RPA solutions though training, tool kits, and templates to effectively identify, evaluate, and mitigate risk — Identify and integrate risk and controls early in the solution development life cycle (SDLC) — Develop and test bots (control design and operating effectiveness)	— Provide risk oversight and support identification, evaluation, mitigation, and, as appropriate, risk acceptance — Establish key risk indicators (KRIs) for ongoing operation of the RPA program — Monitor and manage RPA program changes and monitor for impact to key controls and compliance — Perform continuous risk and control monitoring, optimize based on insights	— Provide RPA risk oversight and support in risk identification, evaluation, mitigation, and, in some cases, risk acceptance — Champion RPA solutioning control better practices — Provide RPA standards assurance through periodic reviews and audits — Monitor KRIs and identify improvements collaboratively

Tuned to company risk appetite, appropriate RPA controls are integrated to help achieve compliance, maintenance of acceptable risk position, and proactive monitoring for improvements.

KPMG

Summary of key messages from ‘Audit of AI & RPA’ survey

Survey based on **133 (120)** internal auditors, mostly heads of IT internal audit or head of internal audit

34% (55%) of respondents indicated to have a less than 50% confidence in knowing whether the organisation is using AI technologies

72% (55%) of respondents indicated to have more than 50% confidence that their organisation is planning the use of AI technologies. This includes **25% (15%)** being confident that AI is already being used.

77% (71%) of respondents indicated to not being confident that governance over AI projects is adequate

74% (74%) of respondents indicated not being involved in managing the organisation's risks around AI

76% (94%) of respondents indicated that IA should be involved in managing the organisation's risks around AI

98% (97%) of respondents indicated that the organisation's AI solution should be subject to internal audits

83% (84%) of respondents are unclear of their audit approach for audits on AI solutions, with **8% (5%)** being totally clear on their approach

Survey questions – Where are you?

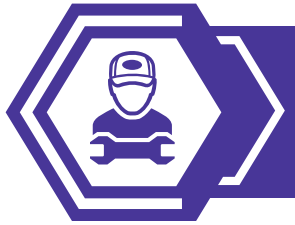
	Survey questions	Don't know	0%	25%	50%	75%	100%
1	How certain are you that you would know about the organisation's use of AI?					▲	
2	To what extent do you think your organisation is planning to use AI?					▲	
3	To what extent do you think AI is already used in your organisation?		▲				
4	To what extent are you comfortable with the governance over these AI projects?			▲			
5	To what extent are you involved in terms of identifying and managing the associated risks?			▲			
6	To what extent should you be involved in terms of identifying and managing the associated risks?					▲	
7	To what extent should AI projects be subject to internal audits						▲
8	To what extent are you clear on your audit approach for these audits?			▲			
	Absolute scores	**No**	**2016**	**2017**	**2018**	**Beyond**	**Total**
9	Do you plan to include an audit on AI solutions as part of your audit plan and if yes for which year-end?				▲		

Questions for internal audit

Do I know where AI is being operated/explored already?

Do I know what the risks are, what controls I would require, and how I would audit these?

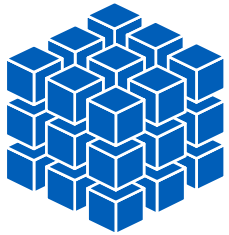
Am I engaged with these projects to ensure my requirements are embedded from the start?



Am I clear on the enterprise's strategy for the three lines of defense, and my role therein?

Questions for internal audit (continued)

Am I influencing that strategy?



Can I clearly articulate my own audit strategy on these topics?

What do I need in terms of people, process and technology to:

A. Enable me to articulate clear requirements to AI programs?

B. Enable me to audit AI development and solutions?

Do I need to pilot "Audit with" to build up my own expertise?

Can I better utilize data analytics to support my evolution?

Wrapping up

We've experienced technology disruption before

Audit skills evolve as technology evolves

Key considerations

- Risk & Governance – Accountability
- Authentication of Bot – Security
- AI Program development and Bot monitoring
- Change control

Plan, Build, Manage = Participate, Participate, Participate

Proactively mange risks by engaging the teams early

Shawn W. Lafferty, KPMG Partner
IT Internal Audit/Risk Assurance

–

April 2018

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia