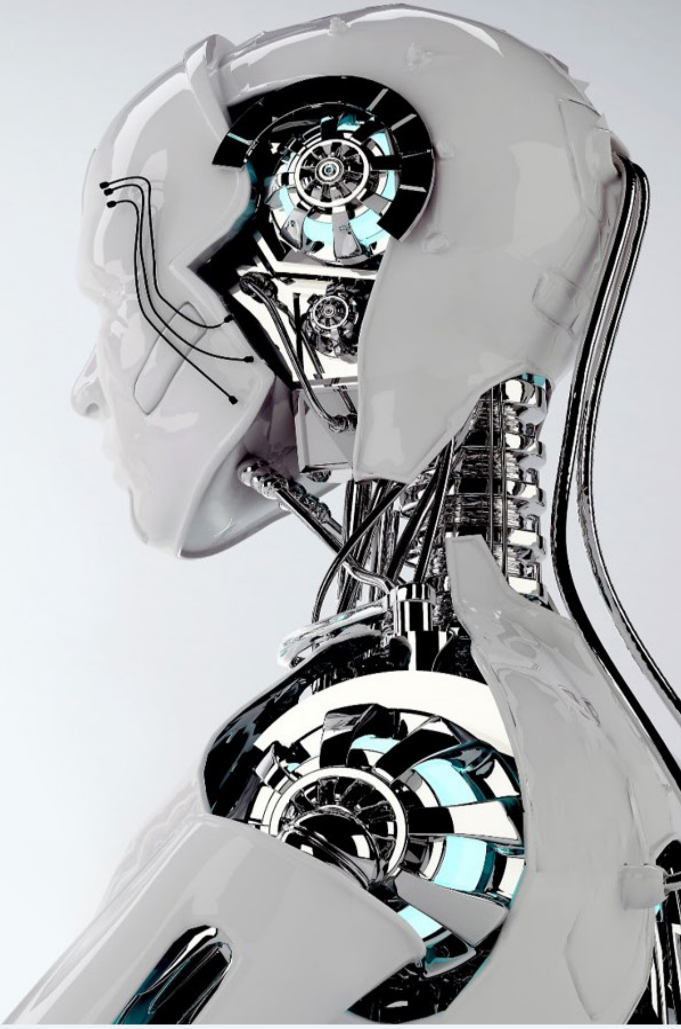
Impact of New Technologies on Audit and Assurance



Todays Digital Footprint

From the 1990s and with the advent of innovation like the Web and digitized content, technology has changed the way we interact with the world – the way we work, shop, bank, travel, educate, govern, manage our health, and even relax.

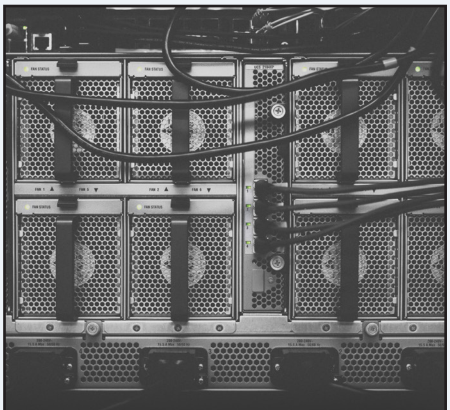
The concept of digitalization is not necessarily new. From the early 2000s, we have seen organizations use technology to gain unprecedented levels of operational efficiency and thus, improve profitability. However, over the past few years, digitalization has gained steam. *Organizations across sectors are being revolutionized by the digital transformation bug.* Drivers for these transformations result from a combination of factors including:

- Changes Impacting products and how they are consumed
- Increased innovation in the technology space
- Availability of low cost devices and thus accessibility of technology to a wide range of individuals.
- Increased availability of data

This means that Companies have had to adopt a "sink or swim" approach to the adoption of varying digital business models to stay relevant.

What does this mean for the Assurance function

Change! The operating model for the assurance function has to continually evolve to meet the needs of the "digital organization". This will require the leveraging of new technologies for optimized outcomes and equipping professionals with the requisite skills and knowledge to identify and manage emerging risks. Key digital trends such as *cloud computing, APIs & ESBs, large data & analytics* amongst other trends are areas that will require focus and knowledge acquisition for the assurance professionals.

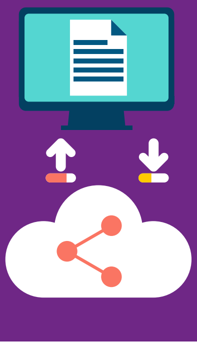


A Forbes Insights survey found 58% of auditors and businesses believe technology will have the single biggest impact on the audit over the next three to five years. And by 2020, smart machines will be a top-five investment priority for more than 30% of chief information officers & business executives.

Impact of New Technologies on Audit and Assurance

Todays Digital Footprint

Cloud Platform



The rise of *cloud based software platforms* is gradually eliminating the need for organizations to host applications within their local environment ('The On-Premise Model'). However, many of such platforms have lesser options for application controls when compared with traditional systems. This lack of control is partly deliberate, to foster an "agile" user experience, partly due to immaturity in the control domain – many of such software vendors have been existing for less than 10 years and simply focused on other strengths than control capabilities. The impact for auditors is that they need to rethink and re-evaluate their approach in providing assurance around cloud systems. This can be achieved by transforming audit approaches leveraging data analytics driven procedures in order to address the less preventive controls in the system. In addition, the processing and storing of data in the cloud for cloud bases systems introduces new challenges around third party management and *data security* and *confidentiality*. These therefore requires the auditors to integrate more *cyber security* capability in the audits.

Key questions auditors must ask on cloud platform

01 How much security is adequate? Is there a need to alter the present security model within the organization?

02 How critical are the applications being hosted? Potential impact of system failure?

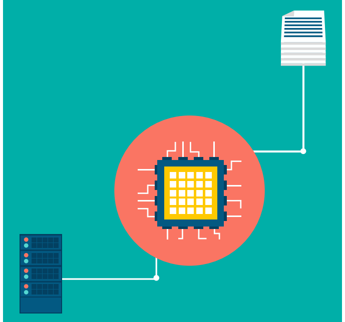
03 How experienced is the outsourcer's with Service Level Agreements and vendor management?

04 What are the applicable country/ regional and industry regulations (e.g., SOX*, IESBA**, GLBA*** and HIPAA****)?

05 What are the cloud vendor's policy on identity, access & vulnerability management?

06 Is there an independent auditor's report on the cloud environment? If so, what does it cover?

Open API/ESB



Application Programming Interfaces (*APIs*) and the Enterprise Service Bus (*ESB*) have significantly transformed the approach for *system integration* and innovative development of software applications, especially mobile applications. The rapid growth and spread of these integration methods can be attributed to the desire for *agility* by reducing time to market for new initiatives - such as new services and capabilities - which will ultimately lead to new revenue streams. APIs and ESBs help achieve this objective by providing a simple, well defined, "Plug and Play" system that scales exponentially. However, with the ease of use and ubiquity presented by these technologies comes increased security risk. Although APIs are not of themselves a security threat, security becomes an issue as soon as end users begin to pull data through requests via these APIs. This is because developers often do not provide enough boundaries to limit *security considerations* from end users in an effort to encourage users and provide useful features and this can inadvertently compromise an *organizations security*.

*SOX: Sarbanes-Oxley Act of 2002

**IESBA: International Ethics Standards Board for Accountants

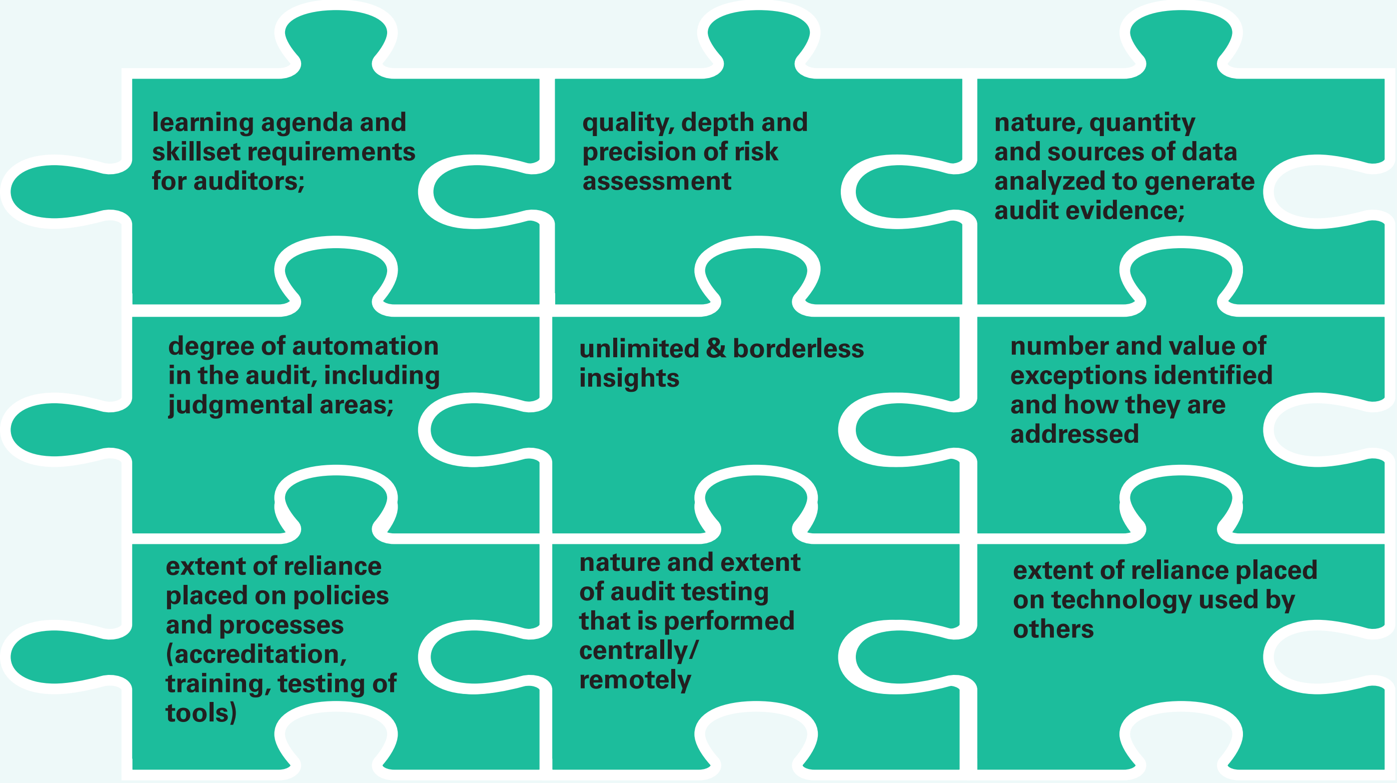
***GLBA: Gramm-Leach-Bliley Act

****HIPAA: Health Insurance Portability and Accountability Act

Data & Analytics

The need for efficiency in business operations is driving many organizations to implement more *standardized and centralized systems*, set up shared service centers, *outsource/offshore* non critical business processes and harmonize critical business processes. The increasing use of harmonized and standardized systems drives the increase of central or centrally accessible data volumes. This gives auditors an opportunity to achieve *a more efficient and higher quality audit*, by transforming the traditional sample based audit approach to centralized and *data driven audit approach* such as 100 percent data population testing by *automated analytical algorithms* instead of sample based testing, thus driving audit quality. The question then arises if current - generally accepted sample based - audit and assurance approaches are still up to par with the vast data volumes and transaction process complexity of the organization.

Key Impact Areas of Data and Analytics



learning agenda and skillset requirements for auditors;

quality, depth and precision of risk assessment

nature, quantity and sources of data analyzed to generate audit evidence;

degree of automation in the audit, including judgmental areas;

unlimited & borderless insights

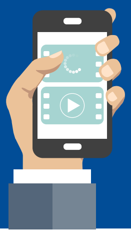
number and value of exceptions identified and how they are addressed

extent of reliance placed on policies and processes (accreditation, training, testing of tools)

nature and extent of audit testing that is performed centrally/ remotely

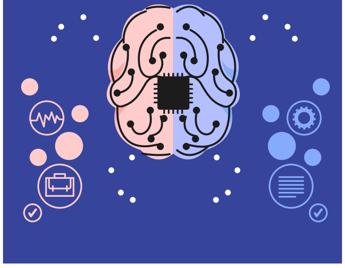
extent of reliance placed on technology used by others

Mobile Application & USSD



Many organizations across the globe have adopted the use of *mobile applications* in putting information at the fingertips of employees making them operate more effectively, enhancing the way people live and work. Also, with the advent of mobile payments based on mobile telephony, the adoption of *USSD* (Unstructured Supplementary Service Data) technology and the range of services supported by this technology has increased significantly over years. Mobile money has done more to extend the reach of financial services in the last decade than traditional "bricks and mortar" banking has in the last century [State of the Industry Report on Mobile Money, GSMA, February 2016]. These advances are made possible by the remarkable progress made in telecommunications technology such as digital technology that integrates transmission, switching, processing, and retrieval of information. However, with new technology evolution comes associated risks - such as user authentication concerns, confidentiality and integrity of information both at rest, in transit and in use - that organizations need to stay on top of to optimize the impact of technology and *mitigate concerns* over its implementation.

Robotics & Artificial Intelligence



Robotics and Artificial Intelligence (AI) are changing business operations and these developments are also open up new opportunities for the audit process itself. A key question that arises is: to what extent (software) robots and artificial intelligence at the client side impact the audit approach?. In the case of clients using software robots in key processes, the auditors will have to gain a certain level of comfort over the reliability of the data processing carried out by the robot. This means that the auditors will need to boost their technology understanding in order to assess the reliability of *robot software.* The profession may be supported by the same digital trend, what if the programming code of the robot can be analyzed by an "*audit-bot*"? AI like *IBM Watson* are able to read, listen, learn and process billions of documents per minute. Such artificial intelligence can work with all relevant standards, including the learning of judgments and other audit considerations, and use this to advise auditors in certain audit questions or challenges.

Impact Areas of Robotics & Artificial Intelligence Enabled Audit

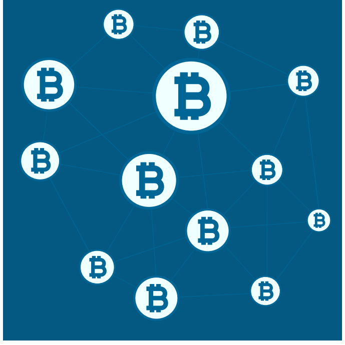
1. QUALITY
Supervised AI systems supports the ability to increase focus on higher value audit judgment

2. INNOVATION
Rapid prototyping and industry relevant procedures

3. LEVERAGE
Artificial Intelligence enable capabilities such as predictive analytics and risk management

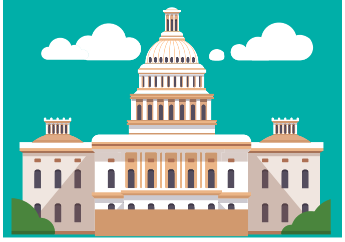
4. INSIGHT
Deriving meaningful insights from previously untapped unstructured data

Blockchain



Currently, businesses and consumers use trusted parties such as banks and telecommunication companies to consummate financial transactions. *Blockchain* allows customers and vendors to connect directly, removing the need for a third party. This concept is currently being adopted by financial institutions in order to drive efficiency in financial transactions, eliminating multiple parties and manual procedures. The risk of *cyber-attack* on a Blockchain is an apparent concern, in addition to the fact that not so many organizations (including regulators) have a full understanding of the underlying technology & model driving Blockchain. The question arises what does this means for the assurance professional? Is there a further need for audit in a block chain supported transactional process? Such questions are yet unanswered and the audit profession will need to form a view and opinion in demystifying the Blockchain environment.

Digital Regulation



While regulators (such as MAS*, ASIC** and UK's FCA***) appear to join investors in embracing the benefits of financial technology innovation, they also acknowledge the new dimensions of *risks* and *challenges* with the emergence of digital business models, especially as it relates to risks that may impact the customer and the overall stability of the financial system. In recognition of the potentially disruptive forces of Digital, regulators are actively pursuing appropriate oversight mechanisms to ensure "*responsible innovation is achieved*". However, regulators globally understand that the approach to regulation and supervision for Digital has to be one that does not stifle innovation and therefore has to be light touch while ensuring that critical risks are appropriately mitigated or managed.

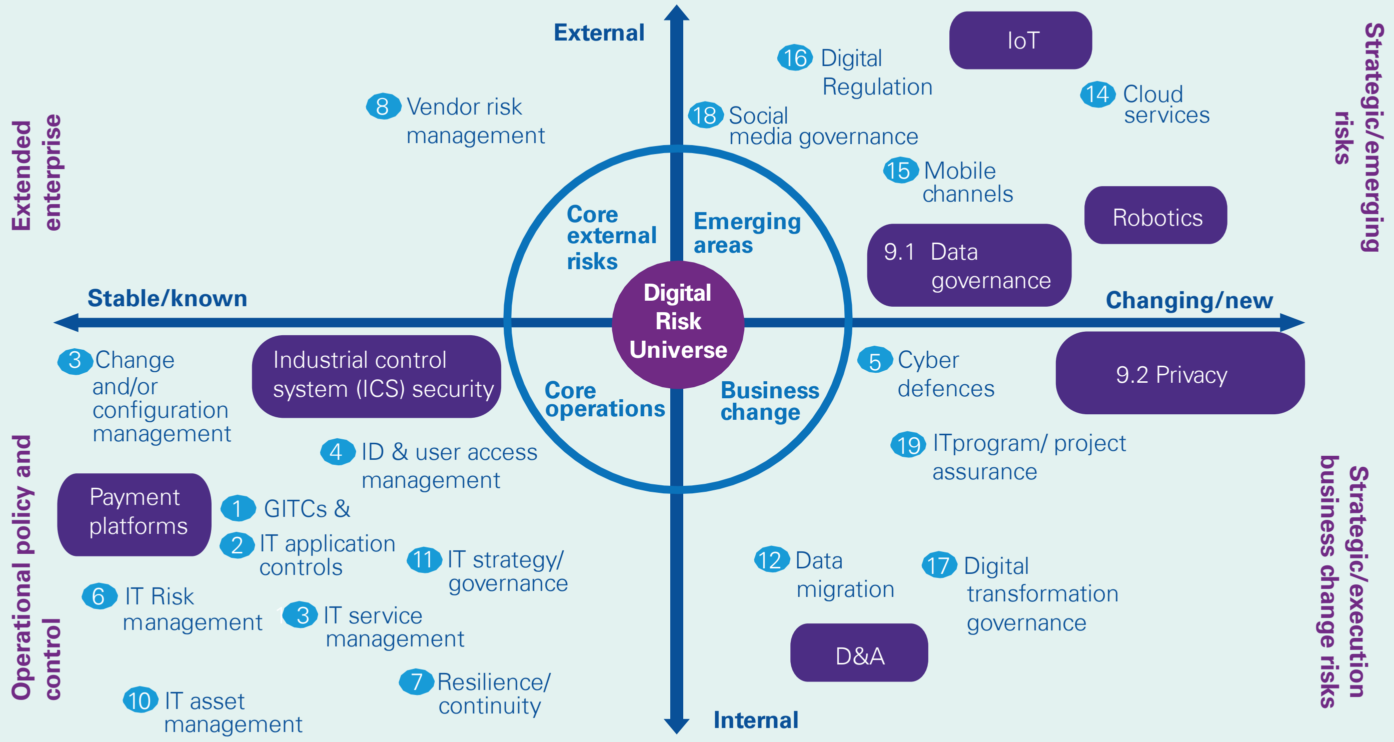
*MAS: Monetary Authority of Singapore

**ASIC: Australian Securities and Investments Commission

***UK FCA: Financial conduct Authority in the UK

The Digital Risk Universe

Based on KPMG's experience from advising clients across sectors on managing technology & digital risk, key risk areas have been summarized in a *Digital Risk Universe*, displayed in the chart below. The horizontal axis depicts the pace of change, from static at the left to fast moving on the right. The vertical axis indicates whether the focus of control tends to be external (above the horizontal axis) or internal (below it).

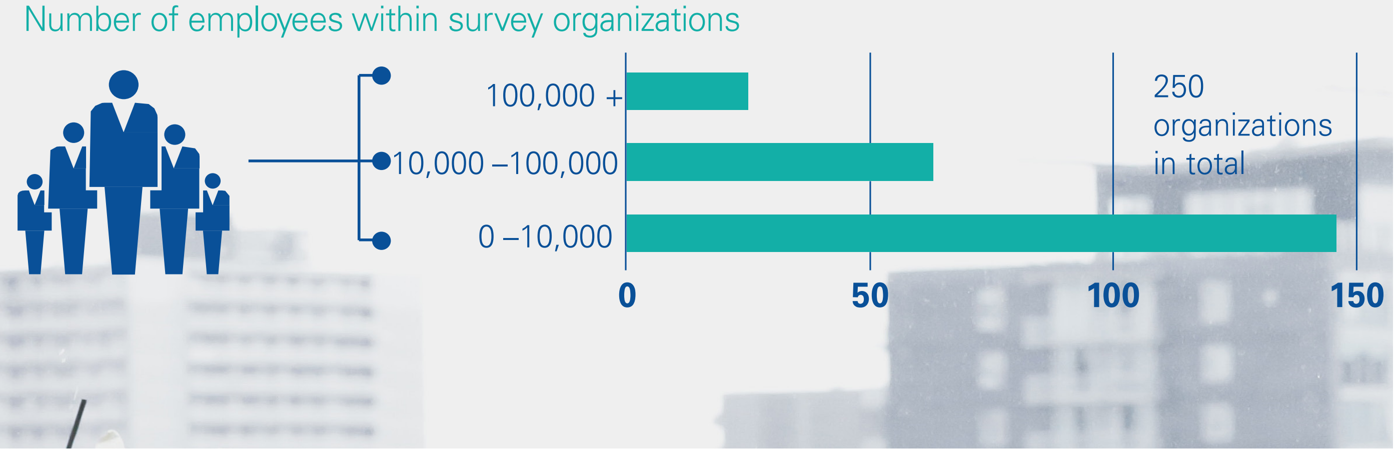


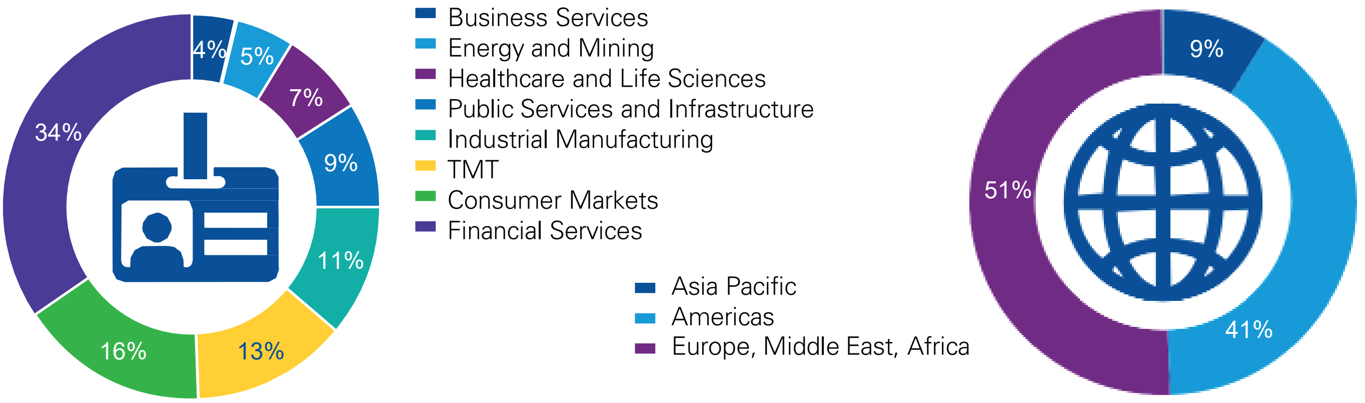
Source: KPMG IT Internal Audit Survey Report: Multiplying risks amid scarce resources, KPMG International, 2017

Excerpts from the KPMG IT Internal Audit Survey 2017

Technology risk is pervasive and continually changing. It is a critical time for technology assurance professionals and IT internal auditors (ITIA), who must build plans to provide assessments of, and insights into, the most important technology risks and how to mitigate them. IT Internal Auditors (ITIA) must keep abreast, and wherever possible anticipate, fast-moving developments in technology. In particular, ITIA must plan, deliver and, when necessary, flex its audit plan in such a way that it responds to these changes in the most appropriate, efficient and effective manner. To find out how ITIA is responding to these challenges, KPMG surveyed ITIA representatives of 250 organizations (see demographic breakdown below). Based on our analysis of the survey results, the some key findings are summarized below.

Number of employees within survey organizations





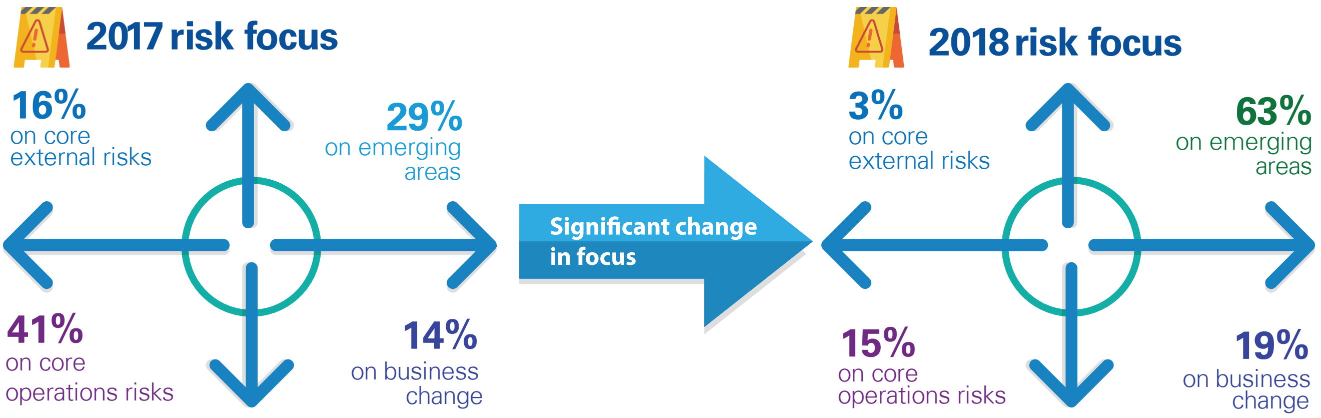
Operating in 8 sectors

Located in 3 regions

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

Focus shifts from core operations to emerging risks

The focus of technology assurance is expected to change significantly in 2018 with emerging risks receiving by far the most attention (63% compared to 29% in 2017), whereas core operations will fall to only 15% (compared to 41% in 2017), lower than business changes. The implication of these findings is that organizations will need to gain access to new skills and potentially invest to leverage new tools to tackle these emerging areas. In addition, companies will have to come up with alternative approaches to providing assurance that take place in real time, reflecting the pace of change of the risk environment.



2017 risk focus

16% on core external risks

29% on emerging areas

41% on core operations risks

14% on business change

Significant change in focus

2018 risk focus

3% on core external risks

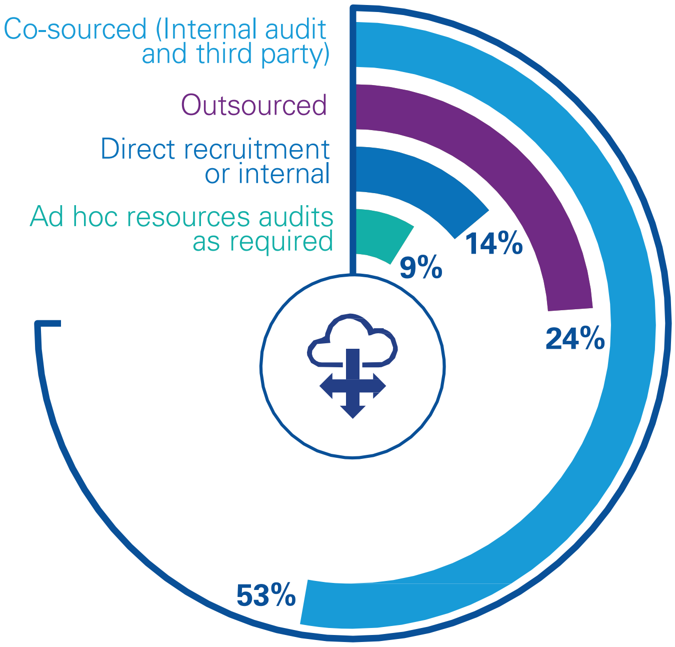
63% on emerging areas

15% on core operations risks

19% on business change

Focus shifts from core operations to emerging risks

Almost no organization has all the IT assurance resources it needs because of the sheer breadth of skills required and the cost of maintaining, training and developing In-house resources to cover all the bases. According to the survey, the main reasons for outsourcing is a lack of people and a deficit of technical skills, the same reasons given in the 2009 and 2013 surveys. In view of the increasing range of risks and the lack of qualified staff, it is not surprising that IT internal audit turns to third parties to fill in the gaps. Although compliance with legal requirements is a highly technical skill for IT internal audit , the survey shows that it is one of the least important reasons for hiring third parties. Given the ever- growing level of regulations around the world, organizations should carefully assess whether they need to think again about regulatory risk.



Priority questions for management to consider

- How effectively do you manage and maintain your **digital content assets**?
- Who is accountable for managing your **digital strategy development and capabilities**?
- How do you procure and manage your **supply chain in a digital delivery model**?
- How effective is your **digital assurance capability**?
- What is your **digital security approac**h?
- How should you best organise your **digital resources**?

KPMG Priority Areas for the Assurance Function

Increased Focus on Knowledge Acquisition and Tooling to ensure that required skills, knowledge and tools are acquired

Increased Use of Data and Analytics to gain insight and provide more recent and relevant assurance to the organization

IT Assurance Co-sourcing: Co-source the IT Audit and Assurance function or hire professionals with technology background

Why Choose KPMG

Our IT Assurance Service Offerings

- ✓ IT Internal Audit
- ✓ Technology Gap Assessment
- ✓ Revenue Assurance
- ✓ IT Risk & Control Assessment
- ✓ COBIT 5 Gap Analysis
- ✓ IT Deal Services (IT Due Diligence)
- ✓ IT Audit Readiness Review
- ✓ IT Regulatory & Compliance Review
- ✓ Technology Roadmap Development
- ✓ Services Organization Control (SOC 1, 2 & 3) Reviews
- ✓ GRC Technology & Control Integration
- ✓ SOD Analytics (Core Banking & ERPs)
- ✓ Software Review
- ✓ Delivery Channels Assurance
- ✓ IT Attestation
- ✓ Real Time System Assessment (RTSA) Assurance
- ✓ IT Contract Compliance
- ✓ IT Policies & Procedures Development
- ✓ IT Post-Transaction Readiness & Integration Assistance

Our Differentiators

- Multi-disciplinary team
- Value-added IT audit & assurance delivery
- Highly skilled IT audit & assurance specialists
- Resources availability (On-Demand)
- Proven track record
- Global reach and support
- Globally Recognized Methodology

Contact Us

Joseph Tegbe
Partner & Head,
Technology Advisory
KPMG Advisory Services
DL: 01 271 0554
Mobile: 0803 402 0989
Joseph.Tegbe@ng.kpmg.com

Boye Ademola
Partner,
Technology Advisory
KPMG Advisory Services
DL: 01 271 8963
Mobile: 0803 402 0983
Boye.Ademola@ng.kpmg.com

Lawrence Amadi
Partner,
Technology Advisory
KPMG Advisory Services
DL: 01 280 9229
Mobile: 0803 535 3082
Lawrence.Amadi@ng.kpmg.com

Kenneth Ukanwa
Manager,
Technology Advisory
KPMG Advisory Services
DL: 01 271 8955
Mobile: 0806 823 8658
Kenneth.Ukanwa@ng.kpmg.com

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Printed in Nigeria.

Publication date: February 2018